HACKER JOURNAL

Anno 1 - N. 14
5 Dicembre/19 Dicembre 2002

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it

Graphic designer: Karin Harrop

Contributors: aDm, Bismark.it, Enzo Borri, CAT4R4TTA, Roberto "dec0der" Enea, Lele-Altos.tk, {RoSwElL}, Paola Tigrino

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00187 Roma - Piazza Colonna, 361-
Tel. 06.69514.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.

Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

CENSURA PREVENTIVA

Ogni tanto qualcuno ci segnala che i link pubblicati sulla rivista portano a pagine inesistenti. Ne abbiamo già parlato in passato: accade che dei testi o dei file che fino a un certo punto sono passati inosservati sui server di qualche provider (magari su spazi di hosting gratuito), grazie alla "pubblicità" ottenuta su HJ, balzino all'occhio per il traffico che improvvisamente cominciano a generare, e vengano rimossi dagli amministratori.

Ma se il sito viene rimosso significa che distribuiva materiale illegale? Non necessariamente. Per esempio, le condizioni d'uso di Digilander su Libero vietano di "fornire informazioni che istruiscano su attività illegali", "memorizzare nel proprio spazio web file di tipo eseguibile", "pubblicare o utilizzare qualsiasi materiale che possa danneggiare il computer di altri utenti (quali virus, trojan horse ecc.)". Stanti queste condizioni, un sito con sole informazioni relative alla sicurezza, o che –parlando di come rimuovere un trojan– includa anche un link alla home page dello stesso, potrebbe essere cancellato. Si tratta di un sopruso? No. Le condizioni sono chiare, e vengono accettate in cambio dello spazio gratuito. Le condizioni sono troppo restrittive? Forse sì.

Lasciando il punto fermo che è vietato distribuire "un programma informatico da lui stesso o da altri redatto avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico" (Art 615 quinquies del Codice Penale), categoria che potrebbe includere qualsiasi exploit e non solo virus e trojan, accade spesso che i siti vengano rimossi anche quando contengono solo informazioni o link. E condizioni simili purtroppo vengono imposte anche da chi offre spazi Web a pagamento.

Negli Stati Uniti, informazioni potenzialmente pericolose e persino i sorgenti di codici di exploit solitamente vengono distribuiti in nome del primo emendamento della costituzione americana, che stabilisce tra le altre cose che il Congresso non può promulgare leggi che limitino la libertà di parola o di stampa. L'esercizio sfrenato del primo emendamento ha anche alcune distorsioni (per lo stesso principio, infatti, non sono vietate le pubblicazioni e le assemblee che si richiamano al nazismo).

Però, in effetti, anche la sensazione di censura di massa che si ha attraversando il Web italiano, ricorda un po' troppo da vicino certi roghi di libri del passato...

grand@hackerjournal.it

Fastweb: coito interrotto



Utilizzo il collegamento in fibra ottica di Fastweb da quasi un anno, e per certi versi mi ha cambiato la vita: niente più sguardi preoccupati al conta scatti durante le navigazioni e le chat, download a velocità altissime, un servizio tutto sommato stabile nel tempo (avrò avuto in totale quattro o cinque giornate di downtime per problemi tecnici o assistenza). Persino le funzionalità di televisione on demand, anche se inizialmente le ho snobbate un po', si sono rivelate comode e funzionali (torno a mezzanotte e voglio vedere l'ultimo TG? Si può fare). Sono quindi un utente felice? Mah, contento sì, abbastanza, ma soddisfatto fino in fondo proprio no.

Da tecnico, sono abituato a cercare di sfruttare al massimo le risorse che ho a disposizione. Non accetto compromessi: se si può fare meglio, si DEVE fare meglio. E tante volte mi soffermo a pensare a quanto di meglio si potrebbe fare con un'infrastruttura come quella di Fastweb a disposizione. Partiamo dal sito: d'accordo che la larga banda consente l'utilizzo indiscriminato di filmati in Flash, ma è proprio necessario utilizzarli sempre, anche per le parti che sarebbero più leggibili in formato Html? Bello, per carità, e molto "affascinante" per i navigatori meno esperti. Peccato che la navigazione nel sito, specialmente alla ricerca di informazioni tecniche, sia difficoltosa e astrusa. Inoltre, il sito è tarato per Explorer in versione Windows, e alcune parti non sono visibili con gli altri browser.

Passiamo ora alla posta. Da un servizio che costa 85 euro al mese, mi aspetto il massimo. Per esempio che la posta sia accessibile anche con il protocollo IMAP, più comodo del POP3 quando sono in viaggio con il portatile. E che offra la possibilità di utilizzare sistemi di autenticazione e download cifrato della posta. E non si tratta di una caratteristica poi così inutile: proprio a causa delle caratteristiche della rete Fastweb, un vicino di casa un po' smanettone potrebbe "sniffare" il mio traffico di rete. Esagero poi se chiedo un server Smtp con autenticazione che permetta di essere utilizzato al di fuori della rete Fastweb?

Vogliamo parlare dei newsgroup? Sul server nntp di Fastweb manca l'intera gerarchia alt.binaries, e tantissimi gruppi accolgono decine di messaggi, mentre su altri server, nello stesso periodo, se ne accumulano a migliaia.

Ma il colmo è una limitazione, a mio avviso assurda, imposta agli utenti. Ciascuno ha in casa un router con tre prese Ethernet, per altrettanti computer (o due computer più la VideoStation per la TV interattiva, anch'essa collegata via Ethernet). Se ho necessità di collegare un computer in più (o magari una delle console con collegamento di rete), devo staccare uno degli altri computer, e fin qui la cosa non è poi tanto grave. Quello che invece è fastidioso, è il fatto che il router si annota gli indirizzi MAC delle schede di rete, e registra il numero di schede che hanno effettuato accessi da quel router in un contatore. Il contatore non si azzera mai, e quando arriva a cinque diverse schede di rete, la linea viene staccata immediatamente. Rifacciamo i conti: posso collegare due computer e la VideoStation; magari un giorno faccio collegare al router un amico che arriva a casa mia con un portatile; un giorno decido di cambiare computer, arrivo a cinque diverse schede e –ZAC!- mi ritrovo senza connessione. OK, chiamando il servizio di assistenza (e attendendo dai 10 ai 40 minuti in linea con la musichetta istituzionale), il servizio viene riattivato immediatamente. Ma qualcuno mi spiega il senso di questa limitazione? Bisogna notare che, se a una delle prese Ethernet del router io collego un altro router con un hub più capiente, niente mi impedisce di collegare decine e decine di computer alla stessa linea, anche se il contratto lo vieta. Insomma, il blocco che interviene se si superano le cinque schede di rete ha effetto solo su chi non rappresenta un danno per Fastweb, e non per quelli che con un abbonamento home collegano l'intera LAN dell'ufficio. Bella policy!

Insomma, con tante risorse a disposizione, ci vorrebbe poco a far davvero felici i propri utenti, invece di lasciarli con il desiderio di quello che Fastweb potrebbe davvero essere.

Gino O. Knaus

UN GIORNALE PER TUTTI: SIETE NEWBIE, SMANETTONI O ESPERTI?

NEWBIE MID HACKING HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un livello di difficoltà: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

HACKER JOURNAL

mailto:
redazione@hackerjournal.it

AUTO ATTACCO

Volevo sapere se potevo attaccare il mio sito per testarne la sicurezza senza creare problemi a nessuno.

Luca

Se si tratta di un tuo server, sì (avviserei comunque il provider di connettività del fatto che stai facendo delle prove).
Se si tratta di uno spazio sul server di qualcun altro, non puoi attaccarlo (perché metti a rischio non solo il tuo sito, ma anche tutti quelli ospitati su quel server). Chiedi all'amministratore del server come puoi fare ad effettuare le verifiche che desideri.



INFORMAZIONE LIBERA

Lavoro in un negozio di informatica, ma personalmente mi occupo di progettare reti in ambienti Win/UNIX e di assistenza. Studio informatica e sviluppo software in ambienti C/C++, VB, Python e altri linguaggi. da un po' di tempo sto scrivendo e raccogliendo alcuni tutorial e veri e propri manuali sulle più disparate argomentazioni. Io avrei intenzione di preparare dei CD e renderli disponibili nel negozio in cui lavoro, magari con un piccolo compenso (1 euro) per ripagare le spese di materiale. Ora mi chiedevo se potrei andare contro una qualche legge che possa recare problemi a me o al titolare del negozio. Potrei correre dei rischi traducendo o creando documentazione free per software proprietario? Per me l'informazione e la possibilità di documentarsi sono delle libertà che nessuno ci può togliere, sicuramente voi siete del mio parere…

senghor

Ciò che scrivi tu lo puoi distribuire come vuoi senza alcun problema, anche se si tratta di documentazione e tutorial relativi a un software proprietario. Per quanto riguarda le informazioni scaricate da Internet o tradotte da articoli già esistenti, devi verificare le disposizioni indicate in ogni materiale. La documentazione del software open source è solitamente pubblicata sotto la licenza Gnu Free Documentation License (www.gnu.org/copyleft/fdl.html), ed è quindi possibile diffonderla senza problemi. In molti altri casi, puoi contattare gli autori per chiedere una liberatoria alla pubblicazione e distribuzione su CD. Probabilmente dovrai sempre indicare la fonte del materiale.

SUL NUOVO SITO

Ho visto che avete aggiornato il sito, e volevo solo segnalarvi che lo trovo un po' troppo lento: sia a casa mia (modem 56k) che da mio padre (ADSL 2Mbit/s) è molto più pesante di quello vecchio.

d4rk elf

Il sito è molto più ricco e complesso, ed è normale che lo trovi più lento con un modem 56k. Con un'ADSL a 2 Mbit però la differenza non dovrebbe essere poi tanta. Forse il problema risiede in un computer un po' troppo lento, o in un browser poco efficiente. La nuova impostazione infatti utilizza tabelle più estese, che possono richiedere qualche secondo di elaborazione in più. Con un computer piuttosto recente non dovrebbero esserci problemi, ma se hai installato Explorer 6 su un vecchio Pentium II potrebbe essere normale un certo rallentamento. Hai provato Opera o Mozilla?

ATTACCHI DI LAMER

Recentemente il mio ZoneAlarm ha rilevato attacchi al mio sistema da parte di qualche Lamer del Ca**o. Vorrei sapere se esiste un programma che riesca a " iniettare " un virus nel Pc di queste spregevoli persone mentre mi attaccano, oppure se posso attaccarli a loro volta.
In fondo non sono scoperti anche loro durante l'attacco?

ReXiD

"Iniettare" un virus? Mica puoi fare le punture ai computer… Scherzi a parte, l'incazzatura è ovvia, ma non puoi legittimamente attaccare nessuno, anche se sta attaccando te. In effetti, tra le tante carenze nella legislazione che riguarda i computer e le reti, c'è quella della "legittima difesa".
Quello che puoi fare è istruire il tuo firewall per rifiutare connessioni dall'IP che hai individuato (e che probabilmente non corrisponderà al vero IP dell'attaccante, se è un minimo sgamato).

PING PONG

Sul numero 12 di HJ, nell'articolo "Toc Toc … chi bussa alla tua porta?", nella descrizione della porta 7 si dice che "è associata al servizio echo … (vero). Viene utilizzata pricipalmente dal servizio PING (falso)".
Per quel po' che ne so, il comando PING non fa uso del protocollo IP e di porte, ma utilizza il protocollo ICMP (la richiesta è un messaggio di ECHO REQUEST, la risposta un ECHO REPLY).

ragi

L'ICMP è considerato parte integrante dell'IP ed è un protocollo per la segnalazione di errori il cui utente principale è l'IP stesso. Il ping è un programma di servizio che sfrutta la porta 7.



MACINTOSH

Perché parlate così poco di Macintosh? Con il nuovo Mac Os X (che non è più tanto nuovo, ed è ormai molto maturo) basato su Unix, ci sarebbero da dire un sacco di cose…

machead

Fondamentalmente, perché quasi tutti quelli

Saremo di nuovo in edicola Giovedì 19 Dicembre!

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

che hanno proposto articoli volevano parlare di Surfers Serials (un database di numeri di serie di programmi commerciali e shareware) o di come modificare suoni e icone del sistema Classic con ResEdit. Io vorrei parlare dell'uso della shell Unix di Mac OS X, dell'installazione di Window Manager alternativi (XDarwin), della compilazione di programmi open source per Mac, della configurazione del firewall integrato, di Linux per Mac, di GnuPG e di Mac On Linux. Tutti i candidati però si sono ritirati appena sentiti questi argomenti. Se qualcuno ha voglia di usare questo spazio anche per i computer con la mela, non ha che da farsi avanti!

PASSWORD DI EXPLORER PERSA

Ho un problema; ho inserito una password per impedire l'accesso ad alcuni siti internet. Credevo che i siti non visualizzabili fossero solo quelli che avevo elencato, e invece mi si richiede la password anche per altri siti non in elenco. Il problema sta nel fatto che ho perso la password e quindi non posso né accedere al sito, né modificare l'elenco dei siti visualizzabili o meno. Ho provato anche a reinstallare Internet Explorer ma non è servito a nulla, perché le impostazioni restano invariate. Cosa posso fare? Potete aiutarmi?

Guido

Occhio: questa procedura prevede di modificare il Registro di Windows. Un'operazione maldestra, può portare al blocco irreversibile del sistema, e alla perdita di configurazione

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: 3sca
pass: strac8

www.hackerjournal.it

IL MURO PER I TUOI GRAFFITI DGITALI

Il sito comincia a riempirsi dei vostri interventi, ma affinché il tutto mantenga una certa organizzazione, è necessario inviare articoli, richieste tecniche e non nelle sezioni più appropriate, e cioè:



ARTICOLI
Vanno nella sezione articoli e saranno pubblicati in home page dopo una valutazione dei moderatori. Per "articolo" si intende proprio un articolo. Molti inseriscono in questa sezione anche richieste e complimenti per la redazione e quesiti strettamente tecnici, ma non è il posto per queste cose.

DOMANDE SULLA RIVISTA O SUL SITO
Problemi col sito, arretrati, abbonamenti, o qualsiasi domanda sulla rivista e sul sito devono essere inseriti nella sezione Faq, che però non è lo spazio giusto per le domande, richieste e quesiti tecnici.

DOMANDE TECNICHE
Problemi, suggerimenti, richieste di aiuto nell'utilizzo del computer e di Internet devono essere inviate nella sezione Sicurezza del Forum, che è divisa in queste sotto categorie:
Newbie: i primi consigli su come rendere sicuro il tuo server/macchina
Pro: sezione rivolta ad esperti o smanettoni...
Linux: tutto sul sistema operativo più bello che esista :)
Inserendo le vostre domande nella categoria più appropriata, e magari con un subject appropriato (non semplicemente "Domanda"), avrete più probabilità che qualche lettore che conosce la risposta vi possa aiutare.

COMMENTI, APPLAUSI E FISCHI
Critiche e apprezzamenti alla rivista devono essere inseriti nella sezione Forum Generale.

e dati. Se non hai mai fatto interventi sul registro, fatti aiutare da qualcuno più esperto. Detto questo...
Dal menu Start scegli Esegui, digita Regedit nella finestra e premi Invio. Nel Registro di Windows, seleziona la chiave

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings

Seleziona l'icona chiamata Key nella parte destra e premi Canc. Chiudi Regedit.
Ora avvia Internet Explorer e vai su Strumenti, Opzioni Internet, seleziona la linguetta Contenuto e fai clic su Disabilita. Ti verrà chiesta una password. Non inserire niente e premi OK. Questo disabiliterà la protezione dei siti (che potrà essere ripristinata con la procedura che hai usato la prima volta).

SUL SOFTWARE IN AZIENDA

Ho appena finito di leggere il tuo utilissimo articolo software pirata in azienda e dal momento che io sono un neo-responsabile di sistemi informativi della mia azienda, un paio di domande hanno immediatamente cominciato a rimbalzarmi insistentemente in testa.
Premetto che io sono solo, ovvero il reparto IT è composto da una sola persona (io) e che l'inquadramento non è stato fatto con qualifica di responsabile (quadro), ma di "addetto" servizi informatici (normale impiegato). Le domande sono le seguenti:
1 Se non ho la qualifica di responsabile, ma di impiegato sono comunque responsabile penalmente delle licenze o è responsabile il mio primo superiore ad essere inquadrato come quadro (quindi in questo caso il direttore amministrativo della catena)?
2 Se metto nero su bianco in una comunicazione al direttore amministrativo (in pratica il mio superiore) la necessità di adeguare le licenze o di rimuovere il software pirata e poi questo non viene fatto, di chi è la responsabilità?
3 Ammesso che si riesca ad avere tutte le 100 postazioni in regola perfetta, il fatto che il mio portatile aziendale "pulluli" di qualsiasi cosa (eh eh) può essere "tollerato" da eventuali controlli della guardia di finanza?

(lettera firmata)

(Ndr: Abbiamo passato la palla a Enzo Borri, che ha scritto l'articolo in questione. Questa è la sua risposta)
Partiamo dalla prima domanda. Il responsabile è una persona FISICA, generalmente chi ha commesso il fatto o, se non identificabile, il legale responsabile quindi: il titolare, amministratore delegato, o legale rappresentante oppure, se dichiarato nelle sue mansioni, il responsabile dei servizi informatici.

Sappi che nella norma chi viene deninciato in questi casi è di solito il titolare e mai un dipendente. Eventualmente se fosse denunciato il tuo titolare, potrebbe rivalersi nei tuoi confronti in sede civile (chiedere un risarcimento). In questa sede si dovrebbe stabilire se tu avevi la responsabilità della cosa e se tu hai una colpa (es non hai mai informato il titolare o chi per esso).
Se, come dici al punto due, tu informi la socetà del problema, puoi dimostrare la tua estraneità ai fatti. Occhio che la tua comunicazione deve essere registrata e "certificata" in qualche modo. Un foglio di carta si può sempre cestinare... L'azienda potrebbe rinadire comunque che tu potevi eliminare il SW copiato La tua risposta in questo caso potrebbe essere: "non potevo farlo per non bloccare il lavoro".
Puoi sempre comunque avvisare la società della presunta irregolarità attuale (magari hanno comprato licenze o multilicenze senza che tu lo sappia...) chiedendo che tu o qualcuno per te faccia una verifica onde valutare la situazione e studiare un piano di acquisto sulla base di ciò che realmente serve.
Riguardo poi al tuo portatile, bisogna vedere cosa intendi con "qualcosa".
Ovvio che se hai un gioco o qualche sciocchezza e si vede comunque che tutto è in regola, credo che la cosa passi decisamente non in secondo ma in terzo o quarto piano... :-)
Ovvio che se inizi ad avere programmi che hanno attinenza col tuo lavoro, l'impressione è diversa quindi anche le decisioni che gli agenti possono prendere sono in relazione ad essa.
Purtroppo, non si può mai dire chi trovi; se trovi il pignolo (è raro ma non impossibile) avrebbe tutti i di-

ritti di procedere.

DIVX SU MACINTOSH

Non riesco a visualizzare correttamente i filmati codificati in DivX con il mio Mac. Ho scaricato e installato i codec per QuickTime da www.divx.com sia su Mac OS 9, sia su Jaguar, ma in certi casi il filmato non si apre neanche, in altri compare con uno schermo bianco, in altri ancora l'audio è completamente corrotto e inascoltabile. Possibile che questi filmati si possano vedere solo con Windows?

Zilves

Effettivamente, le versioni Mac dei codec di DivX Networks sono un po' più scarse di quelle per Win o Linux, e per di più QuickTime è affetto da un fastidioso bug che non consente una corretta decodifica dell'audio. A tutto però c'è una soluzione. Se vuoi continuare a usare QuickTime, puoi utilizzare dei programmi che sistemano i filmati DivX, convertendo il formato in uno più facilmente digeribile da QT. La procedura però è lenta e scomoda.
Molto meglio usare dei player alternativi, spesso "importati" dal mondo Unix. Stiamo parlando di Video Lan Client (VLC) e mPlayer, entrambi disponibili solo per Mac OS X e reperibili partendo da VersionTracker.com.
VLC ha un'interfaccia grafica, può riprodurre filmati in finestra e ha un pannello con i classici pulsanti per la riproduzione, mentre mPlayer è un programma a linea di comando, riproduce filmati solo a schermo pieno, e si controlla con combinazioni di tasti. Se sei per le cose semplici, probabilmente ti troverai più a tuo agio con VLC; se la linea di comando non ti spaventa, e aspiri alla massima qualità, mPlayer è il programma che fa per te. Ah, mPlayer è disponibile anche in una versione con interfaccia grafica, ma funziona solo per la selezione dei filmati e non per il controllo della riproduzione.

☺☺☺ TECH HUMOR ☺☺☺

Inauguriamo qui una nuova rubrica, dedicata alla prolifica satira informatica. Se avete brevi testi o immagini da segnalare per questa sezione, scrivete un messaggio a redazione@hackerjournal.it



Microsoft ha combinato la forza di tre dei suoi sistemi operativi per ottenere Microsoft CeMeNt: duro come una roccia e stupido come un mattone.

NETIQUETTE ALTERNATIVA

1. I verbi avrebbero da essere corretti
2. Le preposizioni non sono parole da concludere una frase con
3. E non iniziate mai una frase con una congiunzione
4. Evitate le metafore, sono come i cavoli a merenda
5. Inoltre, troppe precisazioni, a volte, possono, eventualmente, appesantire il discorso
6. Siate press'a poco precisi
7. Le indicazioni fra parentesi (per quanto rilevanti) sono (quasi sempre) inutili
8. Attenti alle ripetizioni, le ripetizioni vanno sempre evitate
9. Non lasciate mai le frasi in sospeso perche` non
10. Evitate sempre l'uso di termini stranieri, soprattutto sul web
11. Cercate di essere sintetici, non usate mai piu' parole del necessario, in genere e' di solito quasi sempre superfluo
12. Evitate le abbreviaz. incomprens.
13. Mai frasi senza verbi, o di una sola parola. Eliminatele.
14. I confronti vanno evitati come i cliche
15. In generale, non bisogna mai generalizzare
16. Evitate le virgole, che non, sono necessarie
17. Usare paroloni a sproposito e' come commettere un genocidio
18. Imparate qual'e' il posto giusto in cui mettere l'apostrofo
19. Non usate troppi punti esclamativi!!!!!!
20. "Non usate le citazioni", come diceva sempre il mio professore
21. Evitate il turpiloquio, soprattutto se gratuito, porca puttana!
22. C'e' veramente bisogno delle domande retoriche?
23. Vi avranno gia' detto centinaia di milioni di miliardi di volte di non esagerare
24. Trattate sempre i vostri interlocutori come amici, brutti idioti.

NEWS

HOT!

FALLE DI IIS

L'ultimo serio problema di sicurezza relativo ai sistemi Microsoft, classificato come "critical" dall'azienda stessa, consiste in un problema a livello del Remote Data Services del Data Access Component (MDAC), un componente di Windows utilizzato per accedere ai database da parte di varie applicazioni per l'accesso e la gestione di rete, fra cui Internet Explorer e Internet Information Server. Tale falla potrebbe essere utilizzata per la diffusione di worm del genere del famigerato Nimda. La patch è disponibile.

BLU SI FONDE IN TIM

Il 9 dicembre 2002, con un'assemblea straordinaria dei soci, Blu chiuderà definitivamente i battenti, venduta in blocco a Tim. Dopo aver invitato i propri clienti ad aderire alle tariffe appositamente messe a disposizione da parte di Wind, esce definitivamente di scena, dopo una breve e rocambolesca carriera e una lunga e lenta agonia. I suoi asset saranno divisi, come per tutte le spoglie che si rispettano, fra i vari operatori del settore.

VELOCE ED ECONOMICO

Waitec lancerà a dicembre un nuovo masterizzatore della linea Storm, in grado di registrare alla velocità di 52x, dotato inoltre della tecnologia Dds (Dynamic Damping System), che riduce notevolmente le vibrazioni in fase di masterizzazione. Come gli altri della serie, sarà dotato di una versione bundle di Nero Burning Rom. Il prezzo previsto è di 99 euro (Iva inclusa). Altri informazioni sul sito del produttore, www.waitec.it.



PENTIUM 4 A 3 GHZ

È stato finalmente lanciato il tanto atteso Pentium 4 a 3,06 GHz, primo nel suo genere e dotato di una tecnologia integrata che viene annunciata come estremamente efficiente, Hyper Threading. Non si tratta di una novità assoluta: tale tecnologia arricchiva già gli Xeon per server. Ma adesso si tenta il lancio nel mercato consumer, implementando il nuovo processore sui sistemi più noti; fra i primi ad uscire, Dell e Hp.

Il prezzo al produttore (quindi all'ingrosso) dovrebbe essere di circa 500 euro, ma, almeno all'inizio, verrà esclusivamente implementato su Pc di fascia alta (oltre i 3000 euro). Si spera che perlomeno questo possa portare ad un abbassamento di prezzo dei modelli precedenti, e a una reazione analoga da parte di Amd.

Qualche cenno sulla tecnologia: Hyper Threading letteralmente "inganna" il sistema operativo, mostrandogli quello che è a tutti gli effetti un processore unico come se fossero due, e di conseguenza il sistema operativo può affidare al nuovo Pentium due diversi thread allo stesso tempo. Si rivela quindi molto utile per chi gestisce più attività al tempo stesso (scansione antivirus e elaborazione grafica, per fare un esempio). I risultati dovrebbero essere concretizzabili nell'aumento fino al 25% delle prestazioni di sistema.

XBOX ARRIVA IN RETE

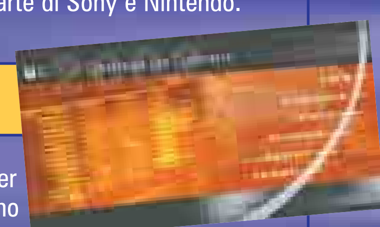
La console di Microsoft ha debuttato ufficialmente su Internet, con il lancio del servizio Xbox Live! (49 dollari all'anno, per ora disponibile solo negli Stati Uniti). Abbonandosi a tale servizio (che è atteso a breve termine anche in Europa) si potrà giocare in modalità multiplayer sul Web, e ottenere due giochi esclusivi e un comunicatore vocale, per conversare via Rete fra giocatori.



E' evidente il desiderio di Microsoft di collocare Xbox in un ambito più ampio di quello della semplice console da salotto, campo in cui sente anche troppo intensamente sul collo il fiato di mastini dell'entertainment, quali Sony e Nintendo. E la recente guerra dei prezzi fra le tre aziende ha visto Microsoft uscire con le ossa rotte, costretta a una politica di vendite sottocosto per non essere tagliata fuori dalla torta divisa altrimenti fra Playstation 2 e GameCube.

Ma gli iniziali insuccessi non sembrano fermare la casa di Redmond, che continua le sue battaglie a suon di pubblicità e immense arene di gioco ad ogni fiera possibile, fino ad arrivare alla nuova avventura in Internet. Non resta che attendere l'analoga iniziativa, già annunciata, da parte di Sony e Nintendo.

LE LEGGI DEL CYBERSPAZIO



Il 28, 29 e 30 novembre 2002, a Bologna, si terrà l'Italian Cyberspace Law Conference (ICLC 2002), organizzato da un consorzio di realtà telematiche e cartacee (la rivista Ciberspazio e Diritto e la comunità NetJus), col patrocinio del Ministero della Giustizia e dell'Ordine degli Avvocati, nonché sotto l'egida del pioniere in questo campo, l'EFF (Electronic Frontier Foundation). A questo convegno si daranno appuntamento tutte le realtà che, in Italia, si occupano di giurisprudenza di Internet e delle nuove tecnologie.

I temi previsti per il dibattito saranno molteplici, ma l'attenzione principale andrà alle istanze riguardanti il diritto d'autore, la privacy, la criptazione dei dati e la tutela dei dati personali, alla ribalta della cronaca anche non strettamente di settore negli ultimi tempi. Si parlerà anche di hacking etico e cracking, tutela dei diritti civili e open source.

Altre informazioni si possono trovare sul sito della conferenza, www.iclc.org.

HOT!

TECNOLOGIA IMPROBABILE



Time Magazine ha stilato una curiosa classifica delle “migliori invenzioni” del 2002, scelte fra i brevetti depositati negli Stati Uniti nel corso dell’anno. Fra questi troviamo oggetti al limite dell’usabile, vuoi per ergonomicità dubbia, vuoi per pura e semplice carenza di richiesta. La palma di oggetto più peculiare, fra questi, può essere indubitabilmente assegnata al “cellulare dentale”, ovvero un dente artificiale, del tutto simile a una comune protesi dentaria, non fosse per il chip racchiuso all’interno che, collegato al microfono e all’antenna incorporati nella struttura, consente di ricevere telefonate (l’autore non si è ancora adoperato a trovare un modo per effettuare chiamate). Ma troviamo anche il “Bowlingual”, che tradurrebbe (il condizionale è d’obbligo) l’abbaiare del nostro cane in linguaggio umano, per farcene capire finalmente le precise esigenze; tale oggetto va per la maggiore in Giappone (quattro milioni di pezzi venduti). E ancora, lo “Sputmik”, un microfono a forma di palla che può essere passato agilmente da un interlocutore all’altro durante un dibattito. Da tenere presente che tutte le invenzioni sono finanziate dal governo americano con borse da 20 a 200 mila dollari.

PRIMO CELLULARE EDGE DA NOKIA



Il nuovo terminale della casa finlandese, Nokia 6200, è il primo sul mercato a supportare la tecnologia Edge. L’acronimo sta a significare Enhanced Data for Gsm Evolution, e si può definire la tecnologia Gsm di seconda generazione, che assieme al Gprs, avrebbe dovuto condurre la telefonia cellulare vero l’Umts. In verità il Gprs, più lento ma più economico, è stato privilegiato, in attesa che i servizi 3G siano pronti al lancio.
Nonostante queste premesse non lusinghiere, Nokia ha lanciato il 6200, cellulare tribanda, che supporta contemporaneamente le frequenze 850/1800/1900 MHz su reti Gsm, Gprs o Edge (che può raggiungere velocità di trasmissione dati di 118 kbps). Oltre a ciò, supporta la tecnologia Java, e può quindi scaricare giochi e applicazioni varie. Ha naturalmente lo schermo a colori, e il supporto ai messaggi multimediali Mms, suonerie polifoniche e radio Fm integrata. Rubrica, Voice Memo e comandi vocali ne fanno non solo un prodotto tecnologicamente avanzato, ma anche uno strumento completo.
Il prezzo finale dovrebbe sfiorare i 350 dollari; la disponibilità prevista in Europa è per la fine del primo trimestre 2003.

CODICI MILITANTI



La casa editrice HopsLibri ha presentato il nuovo libro di Glyn Moody, "Codice Ribelle", dove si racconta la storia del movimento open source dalle origini ai giorni nostri, e l’impatto rivoluzionario che il movimento ha avuto sulla società attuale.
Il principio fondamentale del movimento, come lo racconta Moody, è quello di mettere in atto il libero scambio e in generale la condivisione della conoscenza, a scapito di profitto e convenienza personali. E questo principio diventa storia, attraverso interviste e testimonianze di chi ha fatto la storia dell’open source: Linus Torvalds, Richard Stallman, Eric Raymond, per citarne alcuni. Storia di vittorie e di sconfitte, di scelte azzeccate o errori clamorosi, di successi e di fallimenti.
Per maggiori informazioni si può consultare il sito della casa editrice, `www.hopslibri.com`, dove si possono trovare altri titoli dedicati al mondo della telematica e dell’open source, visti in un’ottica originale e svincolata da luoghi comuni.

COMDEX

Si è svolto dal 17 al 22 novembre, a Las Vegas, l’edizione 2002 del Comdex, una delle più importanti fiere internazionali dedicate alle nuove tecnologie. Protagonista di questa edizione, in tono minore rispetto alle glorie del passato, il wireless, in particolare il Wi-Fi. Ma non sono mancate altre novità, come i Tablet Pc, i computer-lavagnetta sponsorizzati da Bill Gates, accolti con una benevolenza che ha fatto forse dimenticare al manager di Microsoft la delusione per il mancato decoloo dell’accordo con Sendo per il primo smartphone con sistema operativo Windows.

STANGATE PER IL DIRITTO D’AUTORE

E’ in agguato un balzello estremamente dolente, quello per i Cd, i masterizzatori, e i dispositivi e supporti di registrazione digitale in generale. I produttori italiani di elettronica sono in allarme, e si stanno battendo per bloccare la tassa, che, neanche a dirlo, porterà ad un aumento vertiginoso dei prezzi per l’utente finale, fino a far addirittura raddoppiare i prezzi di certi supporti. L’iniziativa, che dovrebbe tamponare i danni causati dalla pirateria, vede l’appoggio di musicisti e produttori, e l’opposizione, a sorpresa, della Business Software Alliance e di vari soggetti istituzionali.

MICROSOFT PERDE

Una notevole falla di sicurezza è stata recentemente scoperta in un servizio Web di Microsoft, a disposizione degli utenti per il download di file e driver e l’upload verso il servizio di supporto. L’accesso a tale area è stata chiusa, dopo che si è scoperto che attraverso quelle pagine si poteva accedere a migliaia di documenti interni all’azienda, nonché all’immenso database degli utenti, con tanto di indirizzi Web e postali, che era protetto da una banalissima password, facilmente superabile.



HOT!

SCOLINUX DISPONIBILE

E' stata aperta la caccia a un gruppo di hacker mediorientali, accusati di avere trafugato una notevole quantità di numeri di carte di credito (si parla di più di 2000 numeri con relativo intestatario e indirizzo), attraverso un worm posizionato in vari siti di ecommerce, che intercettava i dati e li rinviava agli autori. Nulla di nuovo o di originale, tanto più che, grazie al modus operandi molto "professionale" (le operazioni venivano svolte attraverso una complessa catena di proxy) non permette ancora di risalire precisamente all'identità dei pirati, facenti parte del gruppo kuwaitiano "Q8 Hackers", sul cui sito è "regolarmente" pubblicizzata l'azione illegale commessa. Ma l'impresa ha allertato l'Fbi, convinta che i soldi ottenuti da questa truffa così ben organizzata possano andare a finanziare operazioni di terrorismo da parte di gruppi islamici.

Sco Group ha annunciato l'uscita di Sco Linux 4.0 powered by UnitedLinux, un sistema operativo per applicazioni aziendali critiche basato su UnitedLinux 1.0. Tale soluzione può essere definita un vero e proprio sistema operativo Linux di classe enterprise, rappresentando il connubio fra il sistema operativo UnitedLinux di base e il software, il supporto e i servizi di Sco.

Il prodotto è disponibile in quattro versioni: Base Edition, Classic Edition, Business Edition e Enterprise Edition.

Per ulteriori informazioni, consultare il sito aziendale di Sco all'indirizzo www.sco.com.

PRIVACY SUL SERIO

La Guardia di Finanza e gli ispettori del Garante per la privacy stanno controllando minuziosamente il corretto trattamento dei dati sensibili presso la Pubblica Amministrazione. E purtroppo per noi cittadini, le multe stanno fioccando: le violazioni sono molte, soprattutto in merito alla diffusione indiscriminata di informazioni personali di utenti e dipendenti e all'utilizzo non regolamentato di telecamere a circuito chiuso.

CARTOLINE PERICOLOSE

Ha ultimamente preso piede un fenomeno che definire fastidioso è eufemistico, quello dei dialer "truffaldini". Brevemente, si tratta di programmini che, scaricati sotto "falso nome", sconnettono il nostro collegamento dialup a Internet e ci ricollegano attraverso numeri costosissimi. Di solito si trovano simili dialer in siti a luci rosse o dedicati a suonerie e loghi per cellulare; l'ultima tendenza è quella di distribuirli "nascosti" in una cartolina elettronica, o meglio, dichiarare che la cartolina che qualcuno di non meglio definito ha inviato al destinatario potrà essere visualizzata solo attraverso queto "programma". Cosa che effettivamente accade, ma a prezzi che possono arrivare ai 10 euro per chiamata. E spesso il mittente della cartolina non esiste.

Tanto si è parlato dei dialer, della loro liceità o meno, delle scritte a caratteri piccoli che avvertono dei costi e che vengono trascurate dall'utente ansioso di scaricare le suonerie più alla moda; ma quando i dialer si associano a uno spam vero e proprio, i dubbi si esauriscono rapidamente…



DATI PERSONALI ALL'ASTA

Non è più un segreto per nessuno che i dati personali degli utenti siano un tesoro inestimabile per le aziende che fanno marketing su Internet, vista l'avidità con cui vengono raccolti un po' ovunque. E mediamente agli utenti non importa poi più di tanto di dare il proprio indirizzo o parlare delle proprie preferenze a qualcuno, soprattutto se in cambio riceve un gadget o l'accesso a un servizio.

Qualcuno però ci ha pensato su, e ha concluso che non si sarebbe fatto comprare da un cappellino. Ecco così nascere il caso di un trentenne londinese, che ha realizzato un enorme dossier con i suoi dati personali, compresi i più banali e personali (800 pagine di chiamate telefoniche effettuate, liste della spesa, estratti conto e chi più ne ha più ne metta), raccolti in modo minuzioso, e li ha messi all'asta su E-Bay, vendendoli per circa 150 sterline, dopo un lungo rilancio da parte di ben 422 potenziali acquirenti. Non ci si stupisce più di tanto, in effetti, dopo aver saputo che qualche tempo fa qualcuno ha messo all'asta e agevolmente collocato la propria anima…

HACKER O TERRORISTI?

E' stata aperta la caccia a un gruppo di hacker mediorientali, accusati di avere trafugato una notevole quantità di numeri di carte di credito (si parla di più di 2000 numeri con relativo intestatario e indirizzo), attraverso un worm posizionato in vari siti di ecommerce, che intercettava i dati e li rinviava agli autori. Nulla di nuovo o di originale, tanto più che, grazie al modus operandi molto "professionale" (le operazioni venivano svolte attraverso una complessa catena di proxy) non permette ancora di risalire precisamente all'identità dei pirati, facenti parte del gruppo kuwaitiano "Q8 Hackers", sul cui sito è "regolarmente" pubblicizzata l'azione illegale commessa. Ma l'impresa ha allertato l'Fbi, convinta che i soldi ottenuti da questa truffa così ben organizzata possano andare a finanziare operazioni di terrorismo da parte di gruppi islamici.



PDA LINUX ECONOMICI

E' arrivato sul mercato uno dei tanto annunciati Pda con sistema operativo Linux, PowerPlay III (PPIII), che, nella più corretta etica linuxiana, non si fa forte di sofisticatezza e glamour, ma è essenziale, solido e, quel che più conta, economico. Infatti bastano 99 dollari per portare a casa qualcosa di molto simile a un Palm IIIxe con 2 MB di flash Rom, 8 MByte di RAM, Cpu DragonBall da 16 MHz, display monocromatico retroilluminato e una corposa suite di giochi, applicazioni e utility di sistema. C'è da dire che per ora questi sono i soli software disponibili, ma la dotazione non lascia certo a bocca asciutta.
E' in arrivo anche il molto atteso Yopy di G.Mate, un palmare di fascia alta (apparentemente in concorrenza con i modelli PocketPc), con Cpu StrongARM da 206 MHz, display Tft a colori, 64 MB di Ram, 16 MB di Rom, slot di espansione Multimedia Card e jack per microfono e cuffie. Il prezzo dovrebbe aggirarsi attorno ai 450 dollari.



LA RETE ALLO SBANDO

I giorni successivi al Social Forum sono stati a dir poco incandescenti, per i militanti della rete: arresti, sequestri, monitoraggi. Il fuoco incrociato è molto pesante: a accuse di sovversione si risponde con denunce di censura e netstrike. Le realtà telematiche antagoniste sono in subbuglio, dopo i provvedimenti di custodia attuati nei confronti di alcuni dei leader meridionali del movimento, e ancora una volta non vogliono arrendersi, di fronte a questa ulteriore raffica di provvedimenti. I giorni del G8 non sono lontani, e l'atmosfera di questi giorni li ha fatti sentire come sempre attuali: partendo da Ecn, realtà virtuale di aggregazione del movimento, un netstrike, volto alla richiesta di liberazione dei militanti arrestati, ha colpito il sito del Ministero di Giustizia, a sottolineare come gli strumenti prediletti dalle realtà agonistiche siano sempre e solamente "tecnologici" e non violenti, in difesa di una arbitraria repressione.

ALICE ADSL E' FUORILEGGE



Un gruppo di provider, raccolti principalmente nelle associazioni Aiip e Assoprovider, e fra cui spiccano Fiscali, Albacom e Mc-Link, crea fronte comune contro Telecom Italia, chiamando in loro difesa le istituzioni. L'accusa è quella, non nuova per Telecom, di impedire la concorrenza nel campo delle offerte broadband, danneggiando da una parte i concorrenti e dall'altra l'utente finale, che vede così limitate le proprie possibilità di scelta.
Nel mirino dei contestatori, le offerte "Alice Lite" e "Alice Time", riguardanti rispettivamente una connessione Adsl a 256 kbit/s forfettaria e a consumo, nonché Alice Mega, a 1,28 Mbit/s, offerte, secondo i termini della denuncia, sottocosto rispetto ai prezzi del mercato, e in generale effettuate approfittando della posizione prevalente di Telecom nel mercato, senza dare la possibilità ai concorrenti di operare offerte simili. La richiesta è, appunto, quella di rivedere le tariffazioni, sia all'utente finale che nell'ambito wholesale, in modo da consentire a tutti i provider di offrire soluzioni effettivamente concorrenziali.

HOT!

ATTENTI AL MINORE

In Gran Bretagna sta per prendere il via un corpus di legislazioni, annunciate come misure antipedofilia e destinate a modificare i comportamenti dei "chattatori". L'iniziativa più importante è quella volta a rendere reato penale l'attività definita, in inglese, "grooming", intraducibile, ma corrispondente, suppergiù, a tutta una serie di relazioni epistolari "elettroniche" in termini "affettuosi", se indirizzate a minorenni, veri o presunti che siano.

IL CD ONLINE NON TIRA

Nei primi nove mesi del 2002 le vendite online di Cd sono scese vertiginosamente rispetto all'anno precedente, con una perdita di clienti potenziali pari a circa il 25%, a seguire il trend negativo di tutto il mercato discografico. Nel mirino, naturalmente, i circuiti P2P, accusati di togliere mercato alla musica "legale".

WIFI DA RATTOPPARE

Wpa (ovvero il tanto decantato WiFi Protected Access) non è bastato ad assicurare un buon livello di sicurezza al tanto tormentato protocollo WiFi. I tanto temuti attacchi DoS continuano, e, per aggiungere al danno la beffa, Wpa apre la porta a un nuovo tipo di attacco: dopo aver ricevuto in un brevissimo intervallo di tempo due pacchetti non autorizzato, il sistema si disconnette, per sottrarsi all'attacco.



INTERVISTA AL PIÙ FAMOSO PHONE PHREAKER DELLA STORIA

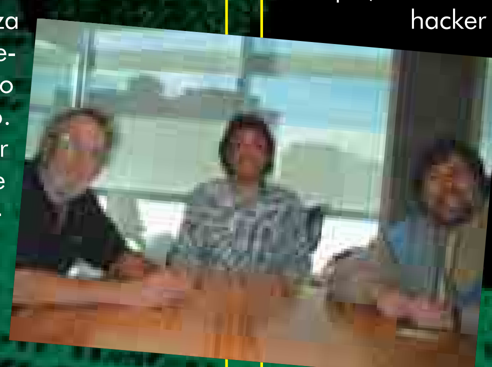
LE SCATOLE MAGICHE DI CAPITAN FISCHIETTO



Parla John Draper, l'uomo che con un fischietto divenne Captain Crunch, il primo hacker del telefono.

Dopo essere passato dall'altra parte della barricata Captain Crunch, il primo hacker telefonico della storia, si prepara a sfidare con la sua nuova invenzione chiunque tenti di violare un sistema informatico. La scatola delle meraviglie questa volta si chiama "crunch box" (**www.shopip.com**), un sistema di sicurezza che riunisce il meglio in fatto di misure anti-hacker. Captain Crunch, al secolo John T. Draper, è arrivato fin qui dopo un lungo cammino. Tutto inizia nel 1971 quando Draper apprende da un cieco che, fischiando vicino alla cornetta del telefono con il fischietto dato in omaggio con una famosa scatola di cereali (Captain Crunch), si può agilmente bypassare la centralina telefonica della compagnia Bell. Decide quindi di costruire la celebre "blue box", un circuito in grado di riprodurre il suono da 2600 Hz del fischietto e di attivare le chiamate in ogni parte del mondo. Con la fama, nel 1972, arriva anche la galera per aver truffato la Bell. Dopo anni di carcere, dopo essere diventato ricco e poi barbone numerose volte il "capitano" ha infine deciso di combattere dall'altra parte, quella della lotta contro gli hacker.
Questo e altro ha raccontato il grande Crunch che nonostante i 58 anni non ha perso lo spirito di un tempo.

Hacker Journal: Captain Crunch, tornando ai mitici anni Settanta, tu allora eri un "phone phreaker", un pirata telefonico. All'incirca quante telefonate gratuite hai fatto in quel periodo?
Cap'n Crunch: All'inizio, appena scoperto che potevo telefonare ovunque senza pagare un solo centesimo, mi sono fatto prendere la mano. Ho chiamato uno per uno tutti quelli che conoscevo, ma questo è durato pochi giorni. Una volta svanito l'interesse per la novità non ho più fatto chiamate gratuite. Anche perché potevo farne quante volevo e senza violare la legge, conoscendo i centralinisti della vicina base dell'aviazione americana che mi mettevano in comunicazione con qualsiasi parte del mondo.
Alla fine facevo sempre le mie solite telefonate senza usare la "blue box", tanto che la bolletta si aggirava sempre sui 70 dollari. Questo ha giocato in mio favore di fronte al tribunale che mi ha accusato di frode telefonica.



HJ: Tutto è partito dal fischietto dei cereali "Captain Crunch" che, messo vicino alla cornetta del telefono, permetteva di violare il sistema di "mamma" Bell. A quel punto si digitava il numero con la tastierina di plastica che attiva a distanza la segreteria telefonica, e il gioco era fatto. Come ti sei accorto di questa possibilità?
CC: Sapevo da qualche tempo che fosse possibile. Mio cognato, che lavorava in una compagnia telefonica, me ne aveva parlato ma in modo molto vago. In verità non mi voleva rivelare questo segreto per non correre rischi all'interno della sua azienda. Mi sentivo, comunque, al settimo cielo, come un hacker che ha appena ottenuto l'accesso al root di un sistema informatico. Stavo per violare la più importante rete di quei tempi.

HJ: Pensavi di fare qualcosa di sbagliato o no?

CC: Ma figuriamoci, no! Il mio intento non era criminale, non volevo affatto derubare la compagnia telefonica. Ma apprendere come il sistema funzionasse e soprattutto se fosse violabile.

HJ: Quello che insomma dovrebbe fare ogni vero hacker?
CC: Certamente, il mio scopo non erano le telefonate a sbafo, questa è stata solo una conseguenza non cercata. Come ho già detto avevo già il modo di farlo gratuitamente e in modo legale.

HJ: Le autorità, comunque, non erano dello stesso avviso. Dopo la pubblicazione sulla rivista "Esquire" di un articolo dedicato alla "blue box", la polizia ti ha pescato "con le mani sulla cornetta", potremmo dire. Sicuramente quell'articolo, oltre ad attirare l'attenzione di gente come Steve Wozniak e Steve Jobs, allora universitari, ha interessato anche la polizia?
CC: Senza dubbio, ma in modo, direi, indiretto. La "blue box" aveva avuto un certo successo fra gli hacker telefonici. Un giornalista di "Esquire" si è interessato ed è uscito il mio nome. Il reporter ha tentato anche di intervistarmi e io invece che tentavo in tutti i modi di convincerlo a non scrivere quell'articolo. Non è andata così: dopo la pubblicazione sono stati incriminati trenta phone phreakers in tutto il paese. Tutti questi naturalmente mi conoscevano e in breve tempo sono risaliti fino a me.

HJ: Esattamente, come sei stato catturato dagli agenti dell'FBI? Come nel film "Public Enemy"?
CC: Più o meno. Stavo per andare in automobile in un supermercato 7/11 vicino casa, una volta sceso mi hanno arrestato.

HJ: Quanti anni avevi quando sei finito in carcere?
CC: Era il 1972, avevo 26 anni. Ero una sorta di nerd.

HJ: Come sei riuscito a sopravvivere dietro le sbarre?
CC: Sono riuscito a farmi molti amici, soprattutto fra i più duri, quelli che avevano una certa influenza. Facendo naturalmente quello che sapevo fare meglio.



HJ: L'hacker quindi?
CC: Certo. Con un trucco telefonico che permetteva di trasformare le chiamate a carico del destinatario in gratuite mediante una "cheese box". Oltre a questo, modificavo le normali radio FM dei carcerati sintonizzandole sulla frequenza delle trasmittenti usate dalle guardie. Così si sentiva tutto quello che dicevano.

HJ: Non riuscivi, insomma, a star lontano dai telefoni. Nel periodo trascorso alla Apple come programmatore e progettista hai pensato bene di costruire una versione più avanzata della "blue box", chiamata "charlie board".
CC: L'intenzione non era quella di aggiornare la "blue box" ma di costruire un compositore telefonico automatico che potesse funzionare come blue box ma anche come modem.

HJ: E per colpa di una "charlie board" sei finito di nuovo in carcere.
CC: Sì, ma non per colpa mia. Stavo dando una festa per il mio ritorno in Pennsylvania. Fra gli ospiti c'erano molte persone che avevo conosciuto al telefono. Qualcuno si mise a giocare con una "charlie board" usandola come "blue box" e la polizia, naturalmente, stava ascoltando. Da qualche tempo, infatti, il mio telefono era sotto controllo.

HJ: Quelli, comunque, sono stati anni indimenticabili per la cultura hacker, alla quale tu ha dato un grande contributo.
CC: Negli anni settanta gli hacker erano gli studenti di informatica che formavano dei gruppi all'interno delle università. Non facevano come quelli di oggi che io chiamo "click kiddies", che usano programmi creati da altri per entrare in qualche sistema informatico. Trent'anni fa ognuno si creava autonomamente i propri strumenti, mettendo mano ai lenti computer delle università per migliorarne le prestazioni.

HJ: La tua ultima invenzione, la "crunch box", è stata pensata contro quest'ultima generazione di pirati informatici?
CC: Più in generale, è un sistema per prevenire le intrusioni in una rete. Si basa sul sistema operativo open source OpenBSD. Chiunque può andare sul sito dell'azienda, registrarsi e simulare un attacco per capire come funziona.

HJ: Pensi di aver tradito lo spirito hacker passando dall'altra parte?
CC: Per me hacker significa una persona che tenta di attaccare un sistema informatico per provarne la violabilità. Io sono sempre stato e continuo ad essere una di queste persone. La pressione degli hacker spinge le aziende a migliorare i propri sistemi, tenendoli sempre aggiornati. Vengono individuate le falle prima che diventino veri e propri problemi.

HJ: C'è qualcuno che comunque non è d'accordo con questa visione, in particolare i governi che anzi rinforzano continuamente le leggi contro la pirateria informatca. Negli Stati Uniti gli hackers, dopo l'11 settembre, rischiano pene fino all'ergastolo.
CC: Ritengo che ci siano ben altri pericoli cui pensare in questo momento, e per i quali andrebbero utilizzate tutte le risorse tecnologiche possibili, come per esempio i terroristi che compiono atti di sangue.

Alessandro Carlini

COME ELIMINARE LE PUBBLICITÀ DALLE PAGINE WEB

NIENTE BANNER, GRAZIE

Passata l'era in cui le aziende Internet si sostenevano solo grazie a finanziatori e ricavi di borsa, tutti sono alla ricerca di soldi. E inseriscono pubblicità in ogni angolo delle pagine.

Purtroppo si tende a perdere sempre di più il senso dei contenuti sul web, ovvero si è passati da un'impostazione quasi prettamente culturale/tecnica/sperimentale a una sempre più orientata al business, con tutti gli inevitabili disagi che questo implica. Navigando sul web si soffre molto questa intrusività, rappresentata da **un vero e proprio bombardamento di pop-up, banner, applets e quant'altro**. I quali il navigatore, malgrado tutto, è costretto a subirne le velleità informative; anche se tale profusione di dati comporta un particolare problema di privacy tutto da scoprire, il principale danno è rappresentato da un vero e proprio overload di informazioni, annunci e proposte, perlopiù pubblicitarie, che vengono indistintamente ed arbitrariamente visualizzate sul proprio browser. **E in mezzo a tanti strilli, immagini lampeggianti e loghi in movimento, trovare le informazioni che si stanno cercando non è sempre così facile.**

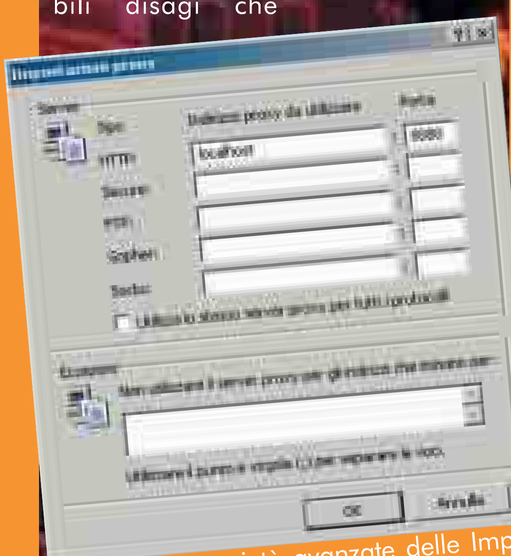


Figura 1 - Proprietà avanzate delle Impostazioni Server Proxy della connessione in Internet Explorer 6.0.

>> Che barba!

Una simile situazione può far scaturire una disaffezione verso lo stesso mezzo di comunicazione da parte di coloro che lo utilizzano e, in misura non secondaria, può far sorgere il sospetto di trovarsi più nella "terra dei cachi" che nella frontiera del cyberspazio. Bisogna rilevare, al riguardo, che si dà sempre meno peso all'impiego del web in una prospettiva di innovazione tecnologica mentre si scorge uno sviluppo unilaterale nella direzione di un marketing selvaggio e senza regole (il web come luogo di business) e presentando, sempre e comunque, tali questioni come conquiste o centrali per la crescita della rete. Ma, nonostante questa selva di inestricabili "conquiste", **esiste la possibilità per il surfer di difendersi e di decidere cosa visualizzare sul proprio browser**; difatti la cosiddetta tecnologia del web content filter o semplicemente filter, aiuta a rendere più equilibrate le navigazioni sul web e meno esasperanti le proprie ricerche, svaghi e interazioni.



Figura 2- Impostazioni proxy di Proxomitron.

>> La soluzione!

Il bello del web content filter è rappresentato da una tecnologia semplice e intuitiva e con risvolti molto potenti in termini di prestazioni; in genere si tratta di piccoli programmi che agiscono come una sorta di proxy interno e, quando si visita un sito, non fanno altro che **riscrivere il codice html prima che il browser lo visualizzi**, in questo modo eliminano il codice "spurio" e rilasciano sullo schermo il contesto essenziale; grazie alla versatilità del "linguaggio" html avviene una manipolazione automatica che consente una sua interpretazione più mirata.

Questa tecnologia ha prodotto diversi software (quasi tutti gratuiti) che essenzialmente prefigurano uno scenario di notevole adattabilità all'ambiente in cui vengono eseguiti.

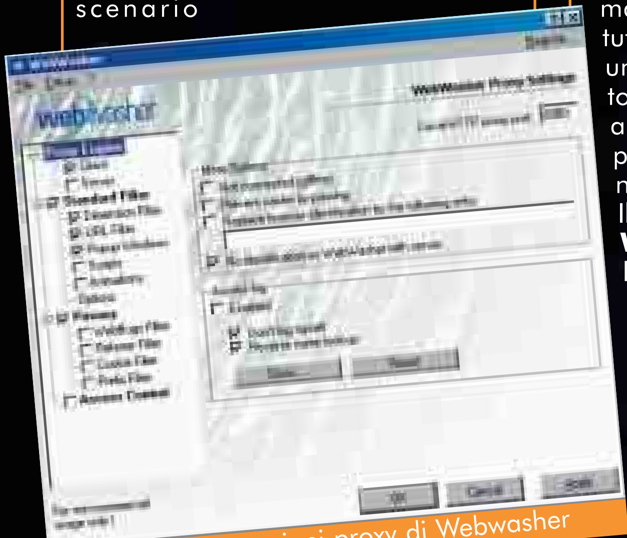


Figura 3 - Impostazioni proxy di Webwasher

>> I programmi

Proxomitron (http://proxomitron.cjb.net) è tra i migliori programmi del genere. È molto personalizzabile e offre una suite di caratteristiche che spaziano dal web content, all'header information, alla gestione dell'animazione delle immagini gif; ed è compatibile con tutti i browser, si caratterizza per una semplice installazione e sul sito, inoltre, si possono trovare filtri ad-hoc creati dagli utenti ed implementarli nella propria versione.

Il più diffuso web content filter è **Webwasher (www.webwasher.com)** meno sviluppabile di Proxomitron, ma non meno efficace e, con una semplice interfaccia user friendly per gli utenti windows, che lo rende un prodotto di semplice utilizzo anche per chi è disavvezzo a "smanettare" con configurazioni o impostazioni di vario genere.

Analogamente **Adsubtract (www.adsubtract.com)** freeware nella sua versione ridotta, si presenta oltre che come buon prodotto di filtraggio, anche come gestore di cookie, nonché con un'interessante opzione statistica su quanti interventi di "pulizia" il programma ha effettuato.

Di diversa natura è invece **Junkbuster (www.junkbuster.com)** meno ortodosso dei suoi colleghi, questo programma è un vero e proprio local proxy, con funzionalità aggiuntive di gestione dei cookie e di filtro; Junkbuster viene eseguito come un "demone" sulla propria macchina (o su una macchina per funzionare da proxy server), mentre la sua configurazione invece risulta essere un po' macchinosa, realizzabile solo con l'ausilio di file di testo e non propriamente immediata nei contenuti; il sito offre, in ogni caso, un'ottima serie di informazioni sulla privacy e su come difendersi dalle insidie imperscrutabili della rete.

>> Come funzionano

Operativamente i web content filter si configurano **sfruttando l'impostazione http dei proxy presente su tutti i browser** (fig. 1) facendo risolvere l'indirizzo web tramite l'indirizzo local loop 127.0.0.1 o localhost ed impostando la porta secondo le indicazioni/adozioni del programma che si sceglie (fig. 2) e (fig. 3), tale impostazione chiama in causa il web content filter ogni volta che si visita un sito (fig. 4) che elaborerà il codice html visualizzando sullo schermo il risultato della sua elaborazione (fig. 5); i programmi, una volta eseguiti, risiedono nella tray area occupando pochissime risorse di sistema. È sempre possibile disattivarli e attivarli senza andare a intervenire sulle impostazioni del browser. **Chi sviluppa siti potrebbe anche usarli per fare il debug delle proprie pagine**: se il risultato in termini performance (velocità e navigabilità) risulterà evidente, significa che bisogna modificare qualcosa.

L'utilizzo dei web content filter potrà risollevare un certo interesse verso il web, come puro luogo d'informazione e di contenuti, introducendo una ventata di libertà digitale che vede il navigatore, non più alla mercè dei siti e delle malizie dei webmaster, ma con una sua partecipazione più consapevole alla navigazione e all'iterattività del web.

Arjuna
arjuna@despammed.com





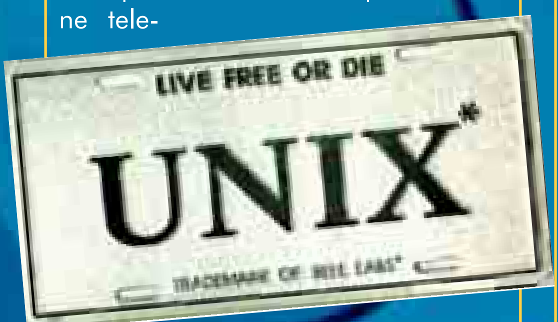
Figure 4 e 5 - Homepage di libero.it con e senza i filtri web attivati. Si noti che vengono eliminate solo le pubblicità, ma non le altre immagini.

BREVE STORIA DEI SISTEMI OPERATIVI UNIX

UNIX E I SUOI FRATELLI

Più appassionante di Sentieri, più intricato dei rapporti di parentela in Beautiful, ecco i più illustri membri della famiglia di sistemi con la X.

Tra il 1965 e il 1969 i Laboratori Bell della AT&T parteciparono, insieme alla General Electric ed al Progetto MAC del MIT allo sviluppo di un sistema operativo multi-utente per centraline tele-



foniche e grossi sistemi di calcolo chiamato MULTICS (MULTiplexed Information and Computing Service). Problemi di budget decretarono però la fine del progetto ma Ken Thompson, uno dei ricercatori della Bell impegnato allo sviluppo di MULTICS, non si perse d'animo e, trovato un 'piccolo' computer Digital PDP-7, si mise al lavoro (sostenuto e aiutato da altri ricercatori della Bell quali Rudd Canaday, Doug McIlroym, Joe Ossanna e Dennis Ritchie) per realizzare un nuovo sistema meno ambizioso ma sempre sulla falsariga del precedente e che Brian Kernighan **chiamò, per un gioco di parole, UNICS (UNiplexed Information and Computing System), poi mutato in UNIX**. Il risultato fu **un sistema di modeste dimensioni ma sufficientemente funzionante e**, soprattutto, in grado di funzionare su hardware poco potente. Visti i buoni risultati ottenuti, furono pertanto trovati i fondi per l'acquisto di un nuovo calcolatore PDP-11/20 e nel 1970 Thompson, aiutato da Ritchie, lavorò per trasportare l'intero sistema operativo su questa nuova macchina.

>> Passaggio al C

Originariamente l'intero sistema operativo era scritto in linguaggio assembly (in pratica un linguaggio di programmazione molto vicino al linguaggio macchina): se da un lato questo garantiva elevate prestazioni, dall'altro **presentava il problema di essere diverso su macchine con microprocessori differenti**. La riscrittura di Unix permise di correggere alcuni errori, migliorando il sistema di base, ma spinse anche i suoi sviluppatori a trovare una solu-



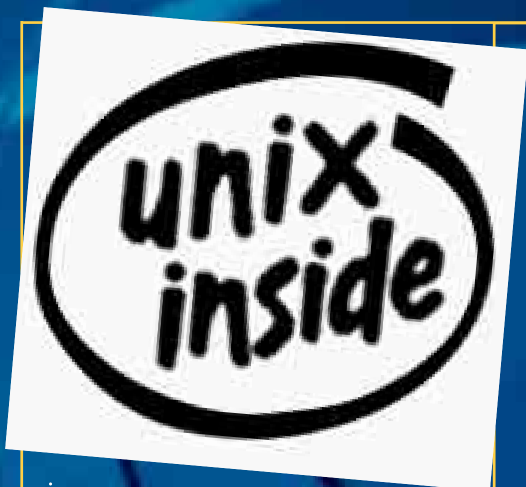
Link utili

I personaggi, le date e i nomi che hanno fatto la storia di Unix
http://www.levenez.com/unix/

L'albero genealogico del ramo BSD
http://www.tribug.org/img/bsd-family-tree.gif

La più completa raccolta di tools Unix liberi
http://www.gnu.org

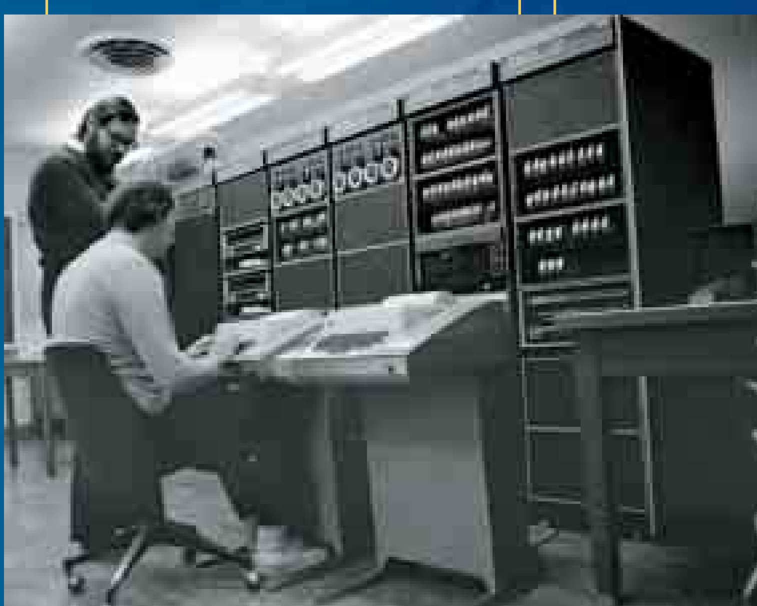
POSIX, lo standard per eccellenza sotto Unix
http://www.pasc.org/



zione per rendere meno laborioso e complicato il trasporto del sistema da una macchina a un'altra (che intanto dovette essere riscritto per funzionare su un nuovo PDP-11/45). Ritchie e Kernighan si rivolsero a Martin Richards, dell'Università di Cambridge, per poter ottenere BCPL (Basic Combined Programming Language), un linguaggio estremamente semplice ma potente per scrivere compilatori che quest'ultimo aveva sviluppato e già utilizzato con successo nello sviluppo di un altro sistema operativo (il TRIPOS). **Una versione modificata di questo linguaggio, che venne chiamata B, servì a iniziare una nuova fase di ricerca e successive implementazioni e ampliamenti portarono al C**. Thompson e Ritchie riscrissero perciò nel 1973 Unix per la terza volta utilizzando però, a differenza delle altre volte, il C e giungendo così a quella che può essere considerata la versione I del sistema. A differenza delle precedenti versioni quest'ultima, essendo stata quasi completamente scritta con il neonato C, era facilmente portabile su nuove piattaforme (i primi ad essere supportati furono i modelli della serie PDP 11/40, /45 e /70). Nell'ottobre del 1973, Thompson e Ritchie presentarono una relazione su Unix al Symposium for Operating System Principles e l'interesse per il sistema esplose.

>> Crescete e moltiplicatevi

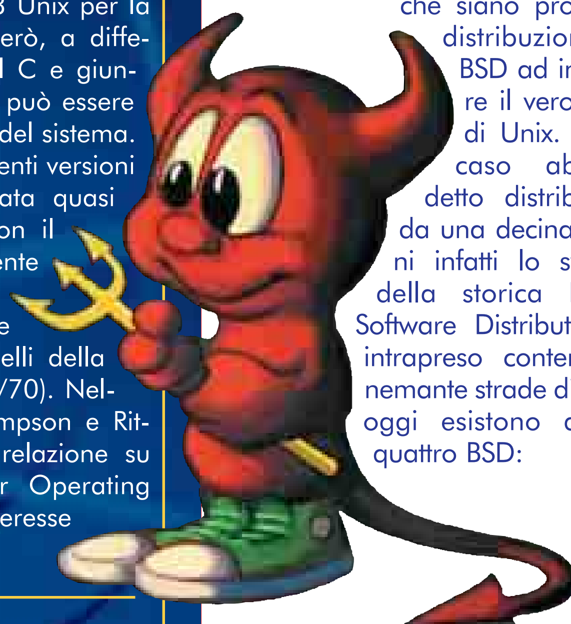
Rapidamente il sistema proseguì nel suo sviluppo e si giunse nel 1978 alla versione 7; nel frattempo AT&T vendette a bassissimo costo la licenza d'uso del sistema ai vari College e alle Università che disponevano di un PDP-11, **diffondendo così Unix in quasi l'80% delle facoltà di scienza dell'informazione presenti sul territorio degli Stati Uniti**. AT&T a quei tempi era però indagata per comportamenti monopolistici e il governo federale non le permise di entrare in competizione nel settore informatico; pertanto le licenze con le quali Unix veniva rilasciato **escludevano qualsiasi ga-**



Ritchie e Thomson alla console di un PDP-11. Ci pensate che quell'armadio è molto meno potente di un PC di oggi?

BSD-FAMILY

La storia di BSD è decisamente affascinante e sono in molti a ritenere che siano proprio le distribuzioni di BSD ad incarnare il vero spirito di Unix. Non a caso abbiamo detto distribuzioni: da una decina di anni infatti lo sviluppo della storica Berkely Software Distribution ha intrapreso contemporaneamente strade diverse e oggi esistono almeno quattro BSD:



FreeBSD
(www.freebsd.org)
FreeBSD è, tra le distribuzioni derivate dal ramo "californiano" di Berkley, quella più nota e utilizzata (anche da aziende del calibro di Yahoo!) ma, soprattutto, la più semplice da installare.

NetBSD (www.netsbsd.org)
NetBSD, anch'essa come FreeBSD derivata direttamente da 386/BSD, è invece un progetto che ha come scopo principale il supporto del maggior numero di piattaforme possibili.

OpenBSD (www.openbsd.org)
A metà del decennio scorso Theo de Raadt, fino ad allora sviluppatore di NetBSD, decise di sganciarsi creando una nuova distribuzione di Net orientata principalmente alla sicurezza; nacque così OpenBSD.

BSD/OS (www.bsdi.com)
BSD/OS, ora di proprietà del Wind River, è la versione commerciale di BSD (la cui sorte appare però incerta).

ranzia, assistenza tecnica, supporto o manutenzione (i sorgenti venivano cioè forniti "as is", così come erano). Questo non venne visto di buon occhio dagli acquirenti ma **costrinse gli utenti a riunirsi per potersi prestare assistenza reciprocamente,** rinforzando i valori che all'inizio avevano portato alla creazione del sistema. Tuttavia proprio questi anni rappresentano un momento cruciale per lo sviluppo di Unix poichè nacquero due filoni fondamentali (e altrettanto distinti): la distribuzione di Berkeley e quella della stessa AT&T.

>> Berkeley non è solo LSD e '68

Nel 1975 Ken Thompson ritornò infatti all'Università della California a Berkeley e portò Unix con sé. Nella facoltà californiana due dottorandi, Chuck Haley e Bill Joy, fecero il porting del sistema Pascal e crearono l'editor di testi vi. **Nacque così la Berkeley Software Distribution di Unix (1978) o, più semplicemente, BSD Unix**: una soluzione che veniva distribuita su nastro su richiesta e le cui stesse intenzioni erano ben lontane dagli scopi commerciali.



Il lavoro a BSD Unix proseguì poi nel corso degli anni e il sistema venne continuamente migliorato e ampliato anche se, nell'ultimo decennio, vi sono state alcune diramazioni dello sviluppo in direzioni differenti; dal canto suo, anche AT&T proseguì lo sviluppo e **nel 1981 uscì Unix System III e, successivamente, Unix System V (1983)**.

>> Dai minicomputer alle workstation

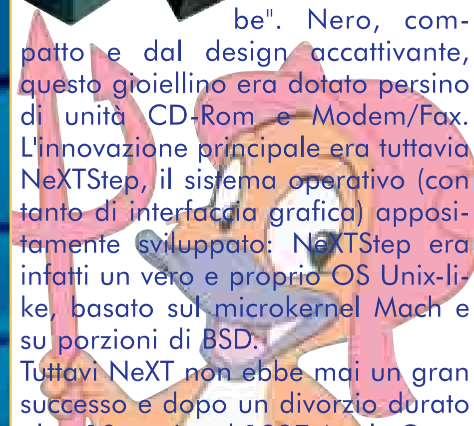
Contemporaneamente, in quegli anni, le nuove workstation, soluzioni hardware più veloci e meno costose dei minicomputer, entrarono violentemente nel mercato e tutti produttori cercarono di offrire la propria versione del sistema operativo Unix o Unix-like, spesso assai lontane dal sistema originale e incompatibili tra loro ma con sigle che in un qualche modo ricordavano l'origine comune. La licenza di Unix venne perciò acquistata da diverse società e lo sviluppo proseguì quindi su binari differenti. Da una parte, **basandosi sulla distribuzione californiana, nacquero infatti NeXTStep e Darwin/MacOSX** (separati da diversi anni ma con un papà, Steve Jobs, in comune :), **SunOS/Solaris** (distribuito dalla Sun Microsystem, fondata nel 1984 proprio da Bill Joy), **SGI Irix, QNX e il microkernel Mach**, originariamente sviluppato alla Carnegie-Mellon University e **utilizzato dal progetto GNU come base per il proprio OS Unix-like HURD. Dall'altra Microsoft Xenix, HP-UX, AIX, Unicos e Minix** si richiamavano invece all'USG System III/V della AT&T; ed è proprio da Minix che discende lo stesso Linux. Ma questa è un'altra storia...

Lele
www.altos.tk

DARWIN: IL QUINTO BSD



Nel 1985 Steve Jobs abbandonò l'Apple, da lui stesso fondata, e creò NeXT, una nuova azienda nata con lo scopo di conquistare il mercato. In pochi anni quest'ultima realizzò una tra le macchine più innovative dell'intera storia dell'informatica: il "NeXT cube". Nero, compatto e dal design accattivante, questo gioiellino era dotato persino di unità CD-Rom e Modem/Fax. L'innovazione principale era tuttavia NeXTStep, il sistema operativo (con tanto di interfaccia grafica) appositamente sviluppato: NeXTStep era infatti un vero e proprio OS Unix-like, basato sul microkernel Mach e su porzioni di BSD.



Tuttavi NeXT non ebbe mai un gran successo e dopo un divorzio durato oltre 10 anni, nel 1997 Apple Computer inglobò la stessa NeXT e Steve Jobs (che pare avere proprio il pallino del "cubo" :) tornò in breve al comando della casa di Cupertino. Il lavoro della NeXT venne perciò ripreso e migliorato per dare finalmente vita ad un nuovo sistema operativo: MacOS X (nome in codice Rhapsody). Ecco pertanto che all'interno della decima versione del SO Macintosh batte Darwin, un vero e proprio cuore Unix che integra molto codice derivato da Free/NetBSD e Mach 3.0 e che è stato reso disponibile (http://developer.apple.com/darwin/) sotto una licenza open source personalizzata (Apple Public Source License).



HARD HACKING

COME RISOLVERE UN BACO DEL SISTEMA DI AUTENTICAZIONE KERBEROS

UNA PULCE A TRE TESTE

Se nella mitologia Cerbero è un cane a tre teste, come saranno fatti i suoi bachi?

Se in questi giorni vi è capitato di navigare nei più noti siti di sicurezza informatica quali Security Focus (www.securityfocus.com) o il sito del governativo CERT (www.cert.org) e centinaia di altri dello stesso tipo, avrete notato il bug che ha messo in allarme il mondo informatico in questi giorni: un buffer overflow nel demone di amministrazione del



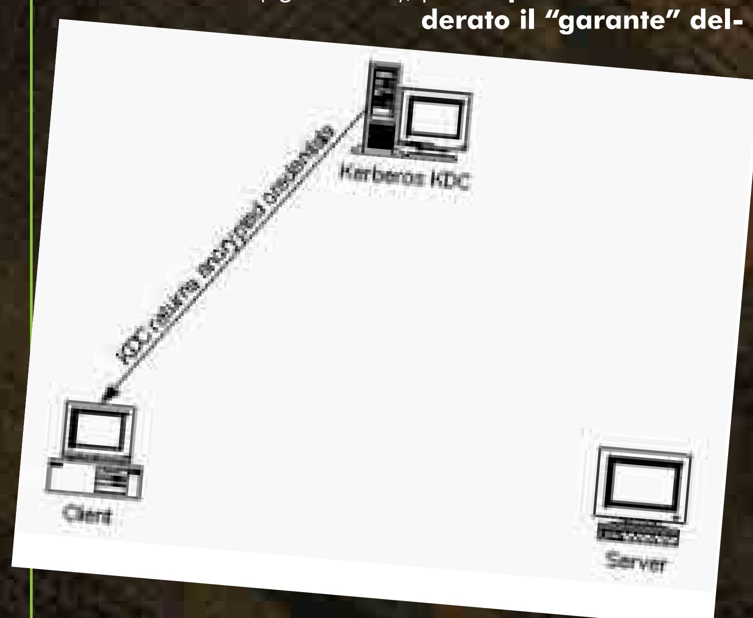
Kerberos. Del funzionamento del sistema di comunicazione cifrata del MIT abbiamo già parlato, seppur superficialmente, in un articolo precedente (n.12 Hacker Journal) a proposito dell'autenticazione di Windows 2000 Server. Questa volta però (strano ma vero) il bug non riguarda l'implementazione Microsoft di Kerberos ma quella della maggior parte delle distribuzioni Linux. Le versioni di Kerberos incriminate sono le seguenti:

MIT Kerberos versione 4 e 5, compresa la krb5-1.2.6;
KTH di eBones prima della versione 1.2.1;
KTH Heimdal prima della versione 0.5.1.

Sono coinvolte anche altre implementazioni che derivino dalle precedenti versioni citate.
Per patchare il bug è consigliabile visitare il sito relativo alla propria distribuzione Linux, dal momento che non tutte sono coinvolte: per esempio la SuSe non sembra avere questo problema.

>> Il nocciolo della questione

Il demone bacato è il kadmin (in alcune implementazioni può avere un nome diverso), che si occupa del cambiamento delle password ed altre richieste di modifica del database del Kerberos, e gira sul KDC (Key Distribution Center) di un sistema Kerberos. Quest'ultimo è, nell'infrastruttura Kerberos, l'elemento più importante in quanto si occupa tra l'altro dell'autenticazione degli utenti e dell'invio agli utenti delle chiavi di cifratura (figure 1 e 2), per cui **può essere considerato il "garante" del-**



la comunicazione Kerberos.



La straordinaria pericolosità di questo bug sta nel fatto che **potrebbe essere utilizzato per raggiungere privilegi root senza bisogno di una precedente autenticazione e quindi senza bisogno di conoscere nemmeno un nome utente o una password validi nel sistema**.

Root: È il livello più alto nella gerarchia degli utenti Unix. Un utente Root può operare qualsiasi tipo di operazione sul computer, senza limitazioni di nessun tipo. Se un malintenzionato riesce a ottenere i privilegi di Root, avrà il totale controllo della macchina.

In altri casi, come ad esempio i noti buffer overflow del wu-ftpd presente in parecchie distribuzioni linux, era necessaria almeno la conoscenza di un account utente. Altra pericolosità sta nel fatto che il bug fa in modo che il sistema restituisca nei log degli errori generici e quindi non facilmente riconducibili a un tentativo di attacco.

>> Andiamo alla "sorgente"

Dal momento che andremo nei dettagli del codice vi consiglio, per seguire meglio l'articolo, di consultare i sorgenti del Kerberos che avete sulla vostra distribuzione nella cartella src/kadmin/ (in alternativa, potete scaricarveli dal seguente indirizzo: http://web.mit.edu/kerberos/www/).



La home page del sito di Kerberos al MIT, raggiungibile all'indirizzo http://web.mit.edu/kerberos/www/

Il file incriminato è il kadm_ser_wrap.c che potete trovare nella cartella src/kadmin/v4server/. All'interno del file si trova la funzione kadm_ser_in(dat,dat_len). A cosa serve? Essa viene richiamata dalla procedura process_client() (il cui sorgente lo trovate nel modulo admin_server.c), che gestisce la comunicazione con gli utenti Kerberos. La funzione kadm_ser_in() riceve in ingresso da quest'ultima, come potete notare dal prototipo della funzione, un buffer (dat) con la relativa lunghezza (dat_len). Sulla seconda variabile (quella relativa alla lunghezza del buffer) non c'è un controllo ossia non viene verificato se essa rappresenti un valore negativo (una lunghezza non dovrebbe poter essere negativa) oppure un valore troppo grande che superi le dimensioni che la memoria alloca alla variabile authent.dat. Ciò permette a un intruso di costruire una richiesta tale da dare alla variabile authent.length (in cui viene riversato dat_len) un valore più grande della memoria allocata per la variabile authent.dat in cui invece viene riversato 'dat'. Questo può fare in modo che la successiva chiamata alla funzione memcpy(), che serve 'riempire' authent.dat possa generare un overflow di authent.dat stessa.



>> L'overflow

La funzione memcpy() riceve in ingresso il buffer dat e lo copia in authent.dat, "tagliandolo" della lunghezza authent.length **che però non è una variabile controllata**; questo può fare in modo che la variabile authent.dat 'vada oltre' il suo spazio di memoria e si ricada quindi nel caso del buffer overflow nello stack. Per risolvere il problema sono state introdotte delle istruzioni di controllo sulla variabile authent.length nonché altre che risolvono problemi relativi al logging degli eventi. Eccovi dunque la patch:

```
Index: kadm_ser_wrap.c
==================================================
RCS file:
/cvs/krbdev/krb5/src/kadmin/v4server/kadm_ser_wrap.c
,v
retrieving revision 1.10.4.1
diff -c -r1.10.4.1 kadm_ser_wrap.c
*** kadm_ser_wrap.c   2000/05/23 21:44:50   1.10.4.1
- --- kadm_ser_wrap.c 2002/10/22 22:07:11
***************
*** 170,183 ****
      u_char *retdat, *tmpdat;
      int retval, retlen;
```

```
!      if (strncmp(KADM_VERSTR, (char *)*dat,
KADM_VERSIZE)) {
        errpkt(dat, dat_len, KADM_BAD_VER);
        return KADM_BAD_VER;
       }
       in_len = KADM_VERSIZE;
       /* get the length */
!      if ((retc = stv_long(*dat, &r_len, in_len,
*dat_len)) < 0)
        return KADM_LENGTH_ERROR;
       in_len += retc;
       authent.length = *dat_len - r_len - KADM_VER-
SIZE - sizeof(krb5_ui_4);
       memcpy((char *)authent.dat, (char *)(*dat) +
in_len, authent.length);
- --- 170,190 ----
       u_char *retdat, *tmpdat;
       int retval, retlen;

!      if ((*dat_len < KADM_VERSIZE +
sizeof(krb5_ui_4))
!       || strncmp(KADM_VERSTR, (char *)*dat,
KADM_VERSIZE)) {
        errpkt(dat, dat_len, KADM_BAD_VER);
        return KADM_BAD_VER;
       }
       in_len = KADM_VERSIZE;
       /* get the length */
!      if ((retc = stv_long(*dat, &r_len, in_len,
*dat_len)) < 0
!       || (r_len > *dat_len - KADM_VERSIZE -
sizeof(krb5_ui_4))
!       || (*dat_len - r_len - KADM_VERSIZE -
!           sizeof(krb5_ui_4) > sizeof(authent.dat)))
{
!       errpkt(dat, dat_len, KADM_LENGTH_ERROR);
        return KADM_LENGTH_ERROR;
+      }
+
       in_len += retc;
       authent.length = *dat_len - r_len - KADM_VER-
SIZE - sizeof(krb5_ui_4);
       memcpy((char *)authent.dat, (char *)(*dat) +
in_len, authent.length);
```

Vorrei indirizzare la vostra attenzione sulle istruzioni "if" evidenziate in giallo, che introducono il controllo dei dati che andranno nella variabile authent.length. Notate inoltre che in caso di errore viene restituito il codice errore KADM_LENGTH_ERROR.

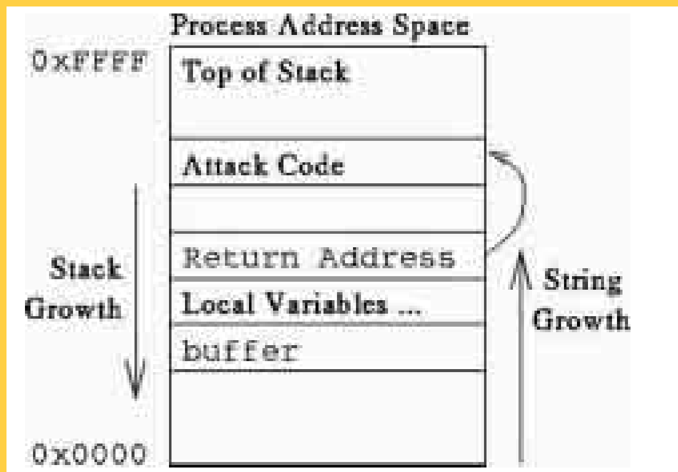
Qualora la vostra versione di Kerberos non abbia queste istruzioni nella funzione kadm_ser_in(dat,dat_len), dovreste provvedere ad aggiungerle e a ricompilare il modulo Kerberos.

Essendo stato scoperto soltanto da un paio di mesi, per questo bug al momento non esiste un exploit specifico. Nonostante questo, i ricercatori del MIT sostengono che nell'ambito dell'hacking statunitense probabilmente un exploit sta già 'circolando' da tempo.

Roberto "decOder" Enea

Il Buffer Overflow

Forse è opportuna una piccola digressione su cosa significhi generare un buffer overflow e



perché lo stack è importante in questo senso.

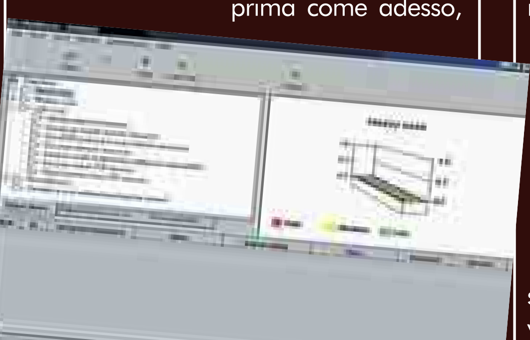
Lo stack (vedi figura qui sopra) è un registro di memoria che ha una struttura dati del modello pila (LIFO). I dati vengono cioè impilati all'interno di esso in modo che il primo dato che viene introdotto è l'ultimo ad essere estratto. Lo stack si occupa della memorizzazione delle variabili locali e degli argomenti che vengono passati a una funzione, nonché lo stato dei registri prima della chiamata alla funzione stessa. Uno dei registri i cui dati vengono salvati nello stack è il registro EIP (Instruction Pointer), che indica alla CPU da quale locazione deve ripartire il flusso del programma dopo l'uscita dalla funzione. Quando in un programma non viene effettuato un controllo sulla lunghezza di una variabile, argomento di una funzione, sia essa generata in locale o in remoto (come nel nostro caso), è possibile che vada a saturare lo stack, andando oltre lo spazio dedicatole e cancellando o modificando il contenuto dei dati adiacenti, come per esempio il Return Address (cioè l'indirizzo a cui deve puntare l'Instruction Pointer dopo l'uscita dalla funzione). Questo, nella migliore delle ipotesi, manda in crash il servizio attaccato generando un Dos; nella peggiore delle ipotesi, l'intruso può modificare il return address stravolgendo il normale flusso dell'applicazione e facendo in modo che il servizio esegua comandi non voluti.

I PRIMI PASSI DELLE PIÙ DIFFUSE TECNICHE DI ATTACCO

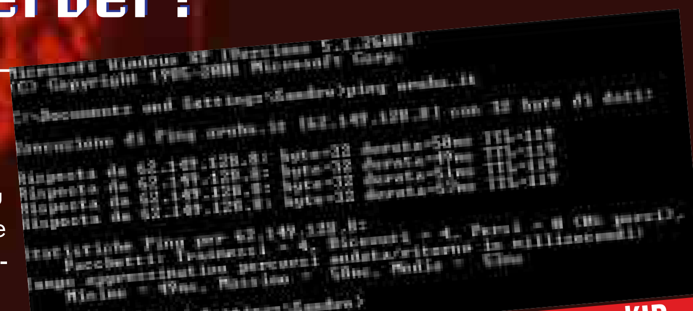
A CACCIA DI INDIZI

Prima di un'intrusione, l'attaccante ha bisogno di reperire informazioni sul sistema. Cosa spiffera in giro il vostro server?

Se per assurdo voi foste degli hacker e voleste entrare all'interno di un sito per dimostrare al suo amministratore, che lo spacciava per inattaccabile, che così in realtà non è, per prima cosa dovreste avere ben chiaro lo scenario che vi si presenterebbe davanti al momento dell'attacco. Lo scenario consiste, ovviamente, nel sistema operativo e nei servizi utilizzati da quel determinato server dove risiedono le pagine da attaccare.
Come riuscire quindi a raccogliere tutte queste informazioni? Esistono, al giorno d'oggi, **un'infinità di risorse per cercare di capire quante più notizie possibili riguardo ai vari server**. Questo è senza dubbio il momento critico di ogni attacco, basti pensare che report di defacement famosi dimostravano che **spesso alle spalle di un'azione di circa 30/60 secondi al massimo, vi erano settimane, se non addirittura mesi, di ricerche incessanti e ripetute**. La scansione dei punti deboli è quindi utilizzata già da molti anni, e prima come adesso, si basa sempre sul medesimo concetto, ovvero quello di interrogare quante più porte possibili per controllare quali di esse siano aperte e ricettive a possibili attacchi. Vediamo a grandi linee quali sono i passaggi chiave per ottenere ciò di cui necessitiamo.



Il NetRecon è uno degli strumenti di scanning più completi.



Effettuando il PING di un dominio si riceve l'IP corrispondente ed altri dati utili da acquisire.

>> Il dominio

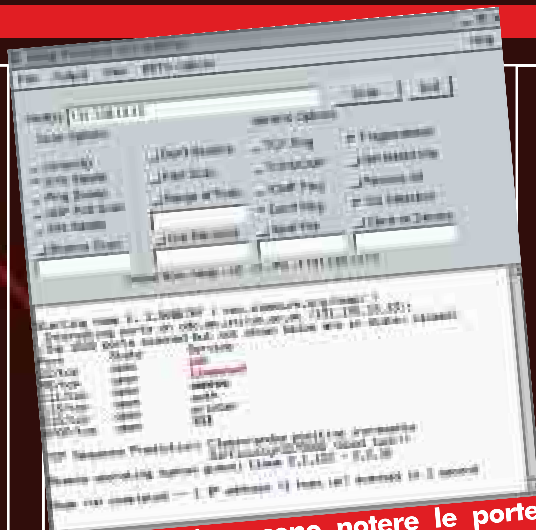
Cercare una specifica rete di internet può risultare abbastanza ostico per l'enormità stessa delle reti contenute. Ci viene in aiuto uno strumento semplicissimo da utilizzare: il whois. È un servizio Internet che, **dato uno specifico account su un dominio, consente di recuperare molte informazioni quali URL o utenti collegati ad esso**. InterNIC è uno degli enti più noti per questo tipo di applicazioni, dato che è l'organo deputato all'attribuzione dei nomi di dominio e degli indirizzi IP.
Dal momento che ho un dominio ed un URL devo utilizzare un altro strumento che mi permetta di reversare il formato alfanumerico mnemonico nell'indirizzo IP associato e, in un secondo momento, controllare che effettivamente quell'IP sia attivo quando pianifico l'attacco. Per effettuare queste due operazioni sfrutto un unico servizio, noto col nome di PING. Non è nient'altro che l'invio di una richiesta ICMP di tipo echo a cui il computer remoto risponde con un pacchetto di tipo PONG, contenente, tra le altre cose, anche l'indirizzo IP del PC stesso.

>> Attacchi "sociali" e attacchi scanning

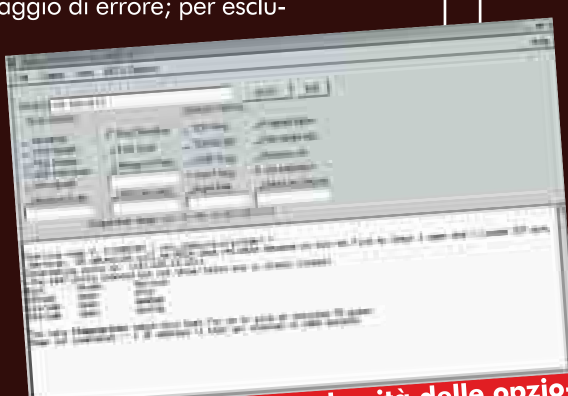
Il social engineering è stato, fin dagli albori della cultura hacker, il metodo più utilizzato per carpire informazioni. Si basa fondamentalmente sulle **capacità personali di rendersi credibile nei confronti di terzi, e sfruttare la fiducia acquisita nel tempo per acquisire privilegi o per "rubare" elementi utili all'attacco**. Vi sarà pur capitato di ricevere email provenienti da account fittizi del tipo assistenza@provider.it che vi chiedono la password della vostra posta elettronica per riaggiornare gli archivi! Tipico esempio di attacco sociale in cui l'attaccante si finge un tecnico. Leggendo queste righe penserete che mai nessuno cada in una trappola simile, e invece le persone che rispondono è di circa il 20-30%!
Gli attacchi di tipo scanning, al contra-

rio, sono basati su pura tecnica, o meglio, su pura tecnologia. Si utilizzano strumenti il cui principio di funzionamento sta nell'inviare pacchetti su determinate porte e vedere quali di esse sono recettive. Esistono molte varianti di questa tecnica; vediamone alcune:

• **Scansione delle porte TCP**: si inviano dei pacchetti e si cerca di stabilire una comunicazione con quella determinata porta; il metodo più semplice e il più utilizzato.
• **Scansione delle porte TCP a frammentazione**: stessa tecnica con la differenza che l'header TCP viene diviso in pacchetti più piccoli, cosicché i filtri di protezione non riescano ad individuare l'attacco.
• **Scansione SYN TCP**: si basa sull'invio di un pacchetto SYN come per aprire una connessione; se il PC risponde con una richiesta SYN/ACK il nostro programma manda immediatamente una risposta RST e chiude così la procedura. Ha il vantaggio di essere quasi invisibile e lo svantaggio di essere molto più lenta della precedente.
• **Scansione TCP FIN**: tecnica ancora più raffinata che si basa sul principio che spesso le porte aperte che ricevono pacchetti FIN rispondono con pacchetti RST facendosi così individuare.
• **Scansione UDP ICMP**: come sappiamo il protocollo UDP non prevede scambio di pacchetti ACK o RST, ma la maggior parte degli host se riceve un pacchetto indirizzato ad una porta UDP chiusa risponde con un messaggio di errore; per esclusione si risale alle porte aperte.



In basso si possono notere le porte aperte e i servizi accessibili da remoto.



Si può vedere la complessità delle opzioni che permettono scanning di vari tipi

>> Gli strumenti del mestiere

Sono moltissimi i programmi di tipo scanner rintracciabili sulla rete, quasi tutti validi e tutti comunque basati sul medesimo principio di funzionamento.
• **Nai CyberCop**: funziona sia su Linux che su Windows; valuta i punti deboli di un sistema facendo la scansione di esso. Riesce anche ad analizzare problemi di sicurezza legati a server ed hub. Integra inoltre una funzione per cui si autoaggiorna da internet scaricando il database dei punti deboli.
• **Symante NetRecon (http://enterprisesecurity.symantec.com)**: è uno strumento operante su Windows che analizza la rete e scopre i suoi varchi, raggruppando i dati raccolti in un report. Agisce simulando vari tipi di attacchi esterni e consigliando come "tappare" eventuali buchi riscontrati.
•**Jackal**: è uno scanner Stealth (nascosto) basato sul principio di funzionamento di tipo SYN TCP.
• **Nmap (www.insecure.org/nmap)**: scanner molto completo che ha la possibilità di lavorare in più modi a seconda della situazione; a volte usa metodologie invisibili, a volte metodologie rapide. Incorpora tutte le metodologie di scanning note.
• **Tiger suite (www.tiger-tools.net)**: è considerato il miglior strumento per la sicurezza delle comunicazioni fra reti. La sua velocità non ha pari con gli altri scanner ed inoltre è l'unico che integri anche le seguenti caratteristiche: network discovery (identifica ed elenca tutti i punti deboli di una rete), local analyzer (scannerizza il sistema locale individuando tra le altre cose anche virus, trojan e spyware), attack tools (set di strumenti che collaudano la sicurezza di un sistema simulando attacchi di varia natura).



Esempio di penetrazione utilizzando il tool TigerSuite

Una volta effettuata la scansione avremo sott'occhio una serie di porte aperte. Sta ora alla vostra tecnica ed alla vostra fantasia cercare di capire come e cosa utilizzare per sfruttare al meglio tali risorse. Nel caso che abbiate effettuato una scansione sul vostro server per controllarne la sicurezza, ricordate che mai nessun computer connesso ad internet, per sua natura, può essere sicuro al 100%. La vostra bravura sta quindi nel tenervi aggiornati sulle più recenti tecniche di protezione e nel metterle in atto cercando così di rendere più alte possibili le mura che circondono la vostra "città".

CAT4R4TTA
cat4r4tta@hackerjournal.it

AGGIORNAMENTO DEI CELLULARI SIEMENS S/ME45, S45I

LA POSTA DAL CELLULARE

Come abilitare il client email sui telefoni Siemens S45 e ME45, con poca spesa e un minimo di fatica.

La nuova versione S45i permette di avere un client email sul proprio S/ME45.

Per iniziare vi serve un cavetto non originale, facilmente acquistabile in internet, oppure se vi va, potete costruirvelo da voi. Ecco i componenti necessari per la costruzione del cavetto:

- 1 circuito integrato max 232;
- 1 zoccolo per integrato a 16 pin;
- 3 diodi 1n4148;
- 4 condensatori da 1 F da 16 V;
- 2 condensatori da 4,7F;
- 1 resistenza da 2,2K Ohm;
- 1 regolatore di tensione 78L05;
- 1 connettore per il cellulare;
- 1 condensatore non polarizzato da 100 nF;
- 1 cavetto seriale per la porta com;
- 1 interruttore;
- 1 basetta millefori 13x10.



Il circuito per il cavetto una volta terminato apparirà così.

Basta guardare le figure 1, 2 e 3 per capire come vanno posizionati i componenti. Una volta terminata la costruzione dobbiamo verificare se il cavetto funziona correttamente, per farlo basta utilizzare il programma SiemensSMS di Silver, che si trova su http://digilander.libero.it/silvestro1977.



Fig. 1 - Lo schema del circuito per realizzare il cavo di connessione.

>> Prima di fare l'aggiornamento

Per eseguire l'aggiornamento, vi serviranno i seguenti programmi:

- SM45Toolsv12, per poter leggere e scrivere la memoria flash;
- un editor esadecimale per poter apportare alcune modifiche alla flash, per esempio XVI32;
- la versione per winsup del firmware dell'S45i, dove potete scegliere la V.03 o V.04 (io ho usato direttamente la V.04).

Realizzate un backup della rubrica indirizzi con Quick Sync, cancellatene il contenuto, e cancellate inoltre tutti i promemoria scaduti.

Per iniziare, **caricate tutta la batteria del cellulare, collegate al computer il cellulare spento e utilizzate il programma SM45Tools**, configuratelo con la vostra porta, modello e Baud Rate a 57600, poi andate nella sezione Read flashread from flash e contemporaneamente premete leggermente il tasto di accensione del vostro cellulare (per pochi secondi senza farlo accendere). Infine salvate la vostra flash. Custodite gelosamente questo backup, **vi servirà a riparare eventuali danni e a poter tornare indietro**.

>> All'opera!

Se tutto è andato bene avrete un backup della memoria, fate partire l'aggiornamento della vostra versione Winsup S45i_040101, configurando la porta seriale e selezionando i due skip che riguardano il pre-check e post-

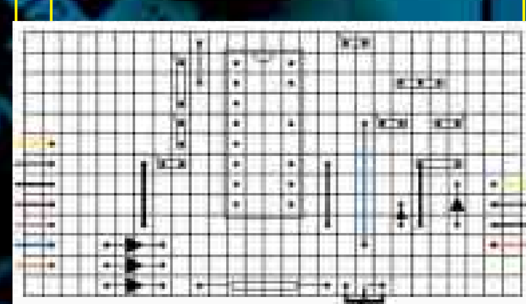


Fig. 2 - Schema dei collegamenti della basetta, parte superiore.

chek, ricordandovi di premere il tasto di accensione del cellulare. Una volta terminata la procedura di aggiornamento del Winsup, riaprite ancora SM45Toolsv12, rileggete di nuovo la flash e utilizzate un programma esadecimale per cambiare i seguenti valori:

```
Offset per firmware vers 04
per disabilitare il primo
controllo CRC
298AE2: DA CC
298AE3: CD 00
298AE4: DC CC
298AE5: 59 00

per disabilitare il secondo
controllo CRC
2DB73A: 2D 0D

per abilitare NetMonitor
2A9156: 2D 0D

Modificare questi byte se
si aggiorna un S45
2CAE46: 76 CC
2CAE47: 50 00
2CAE48: 80 CC
2CAE49: 00 00

Modificare questi byte se
si aggiorna un ME45
2CAE3E: 76 CC
2CAE3F: 50 00
2CAE40: 00 CC
2CAE41: 10 00
```

Per esempio, se usate **XVI32**, per apportare delle modifiche a questo indirizzo **298AE2: DA CC** bisogna:

- apri-

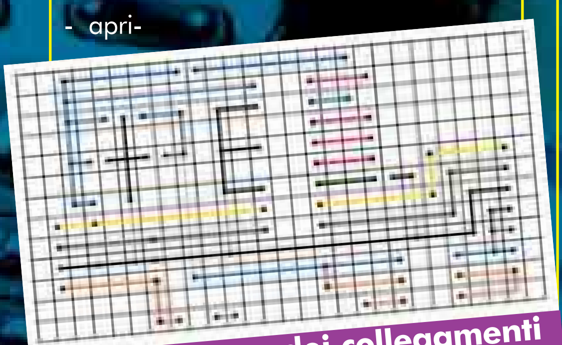


Fig. 3 - Schema dei collegamenti della basetta, parte inferiore.

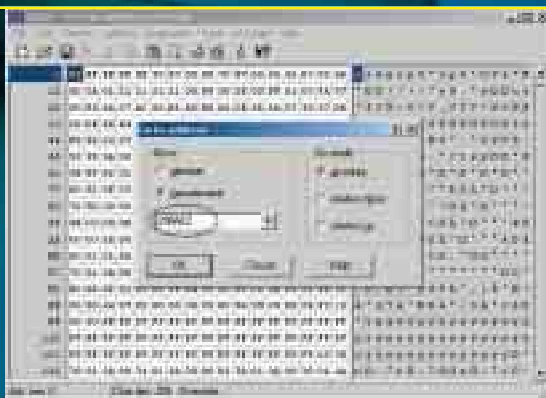


Fig. 4 - Ricerca degli indirizzi da modificare con XVI32.



Fig. 5 - Individuazione del byte da modificare nell'editor esadecimale.

re il file bin;
- controllare che nel menù alla voce **tools** sia selezionato **overwrite**;
- dal menù selezionate: **addressgo tohexadecimal** e inserite nella finestra **298AE2** e premete ok (figura 4);
- il programma trova l'indirizzo di memoria **298AE2** e selezionato c'è **DA** (figura 5);
- non vi resta che scrivere **CC** al posto di **DA** (figura 6);
- una volta fatti tutti i cambiamenti dovete salvarlo con **Save As...**

Quindi terminata la modifica caricate la nuova bin nel cellulare, poi andate nella sezione **IMEIRead Phone** (premete il tasto di accensione),comparirà il vostro **IMEI** ed infine fate **unlock**.

Ringrazio Marcello, Nick, ntc_Silver, Rylos, Lisa e tutti i membri del forum.

KoRn
Issues75@libero.it

LINK UTILI

Se avete domande riguardanti la costruzione del cavetto potete fare riferimento ai siti:
http://digilander.libero.it/thenickside

http://digilander.libero.it/marcelloME45solution/index.html

Trovate ulteriori informazioni riguardanti l'aggiornamento su:
http://www.rylospower.com/public/forum/topic.asp?TOPIC_ID=1964&SearchTerms=RICAPITOLANDO,ME/S45,TO,ME45i/S45i,
E sul canale #X35i_FORUM del server irc.azzurra.net

I programmi necessari possono essere scaricati da:

http://www.gsmiq2000.com/siemens/swup/s45i/s45i_040101.zip

http://web14.xlserver.de/Siemens/Downloads/SM45Toolsv12.zip

http://www.handshake.de/user/chmaas/delphi/download/xvi32.zip

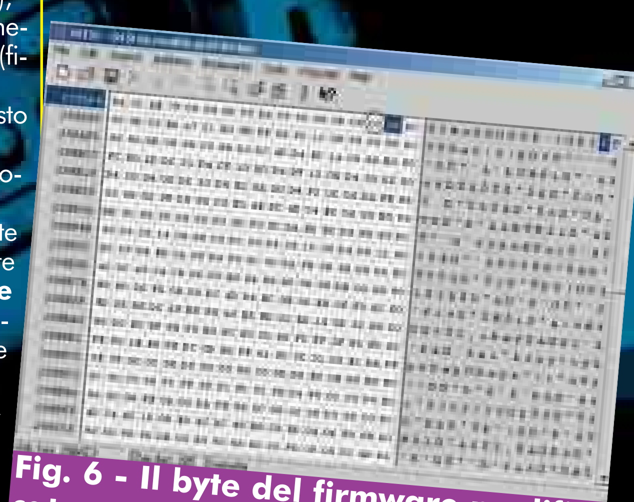


Fig. 6 - Il byte del firmware modificato.

IDENTIFICATION ORDER NO.
5 Dicembre 2002

WANTED

DIVISION OF INVESTIGATION
H.J. DEPARTMENT OF NET
CERNUSCO S.N., MI

Fingerprint Classification

16 0 5 U 001 20
I 17 U 001

KIDNAPING

NOME: Opaserv
ALIAS: W32/Opaserv.worm, W32/Opaserv-A, Win32.Opaserv, Worm.Win32.Opasoft
DATA NI NASCITA: 30 Settembre 2002
DIMENSIONI DELL'INFEZIONE: 28.672 bytes
SISTEMI INFETTABILI: Windows (95/98/NT/2000/XP/Me)
SISTEMI INMUNI: Windows 3.x, Microsoft IIS, Macintosh, Unix, Linux

Chi utilizza un antivirus aggiornato e ben configurato ha naturalmente pochissime possibilità di rimanere colpito da software malevoli ma non si può mai escludere di essere potenzialmente soggetti ad attacchi informatici dall'esterno, soprattutto se si dispone di una connessione a banda larga, se si ha un indirizzo IP fisso e se si rimane connessi ad Internet per lungo tempo. Worm e virus che circolano in Rete sono ancora numerosissimi, sebbene l'aumento degli strumenti di sicurezza tra gli utenti renda loro più difficile moltiplicarsi in modo incontrollato. È dunque necessario non abbassare la guardia. W32.Bugbear e W32.Opaserv: questi i nomi di due worm scoperti nei mesi scorsi e che stanno in queste ore aumentando rapidamente la propria diffusione nei sistemi Windows a causa di alcune proprie singolari caratteristiche. Il Symantec Security Response ha elevato a livello 4 la soglia di attenzione per il primo che è attualmente il più diffuso in Italia ma ne parleremo nel prossimo numero; questa volta concentriamo la nostra attenzione sul secondo.





Danni provocati

Fortunatamente Opaserv non danneggia il sistema colpito in modo significativo. Il worm opera una serie di modifiche al file di registro di Windows che gli consentono di auto-eseguirsi ad ogni avvio del sistema. Infine se ci sono cartelle condivise in rete sul disco C:, Openserv copia sè stesso al loro interno con il nome di file Crsvr.exe. Poco dopo l'avvento di Opaserv è stata realizzata anche una sua variante, W32.Opaserv.E che ha corretto alcune imperfezioni del precedente per renderlo ancora più dannoso.

Metodi di contagio

Capace di infettare tutti i sistemi Windows con la sola eccezione di Windows 3.x, Opaserv è un worm che si diffonde sui network di condivisione dei file, quindi all'interno di sistemi di file-sharing ma anche in reti locali aziendali o private laddove tutte le operazioni non siano protette da password. Opaserv è contenuto nel file Scrsvr.exe che viene eseguito sul computer trasmettendo l'infezione. Una volta dentro il sistema, il worm tenta di scaricare aggiornamenti dal sito www.opasoft.com per renderlo inoffensivi i virus anche aggiornati ma il sito è stato subito cancellato ed ora non è più operativo. Per un incremento della diffusione, la Symantec ha alzato da 2 a 3 la soglia di attenzione per questo worm.

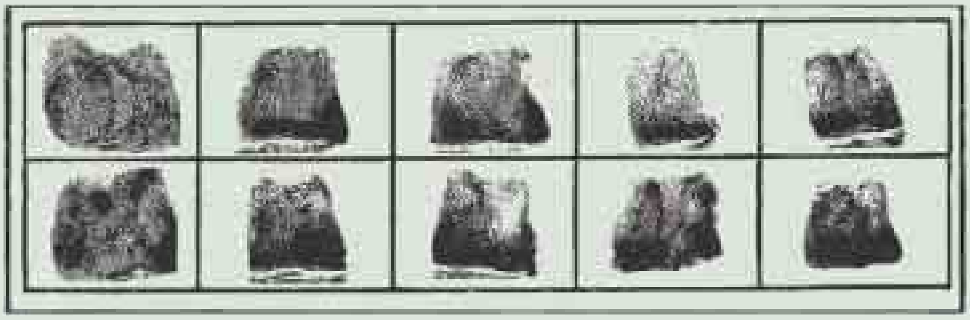
Il worm copia se stesso nel computer infetto in un file di nome Scsvr.exe e apporta alcune modifiche al sistema.

L'esistenza dei file Scrsin.dat e Scrsout.dat nella cartella C:\ indica un'infezione locale e quindi che il worm è stato eseguito dal proprio computer.

L'esistenza del file Tmp.ini nella cartella C:\ indica un'infezione remota, cioè che il computer è stato infettato da un host remoto.

La chiave di registro

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
```



contiene il valore ScrSvr o ScrSvrOld, che è impostato a c:\tmp.ini.
Quando Opaserv viene eseguito controlla il valore ScrSvrOld nella chiave di registro

```
HKEY_LOCAL_MACHINE\Software\
Microsoft\Windows\
CurrentVersion\Run
```

Se il valore esiste, il worm cancella il file a cui ScrSvrOld è diretto mentre se non esiste il worm cerca il valore ScrSvr nella chiave di registro. Se anche questo valore non esiste, il worm aggiunge il valore ScrSvr in C:\Windows\ a quella chiave di registro per poi controllare se viene eseguito come il file C:\Windows\ScrSvr.exe; se non è così copia se stesso in quel file e aggiunge il valore ScrSvrOld <nome originale del worm> alla chiave di registro

```
HKEY_LOCAL_MACHINE\Software\
Microsoft\Windows\
CurrentVersion\Run
```

Dopo queste operazioni il worm controlla i valori del registro e la directory da dove il worm viene eseguito e crea dei valori in modo che ci sia eseguita solo un'applicazione alla volta con l'infezione. Se non è già in esecuzione, il worm registra se stesso in un processo sotto Windows 95/98/Me. Così i computer con sistemi operativi Windows 95/98/Me eseguiranno il worm ogni volta che si avvia Windows poichè il worm modifica la parte [windows] del file C:\Windows\Win.ini aggiungendo la stringa

```
run= c:\ScrSvr.exe
```

Il worm modifica il file C:\Windows\Win.ini dopo aver copiato se stesso come C:\Windows\ScrSvr.exe; di conseguenza gli antivirus troveranno e cancelleranno il file con l'infezione dopo che il sistema è stato alterato, ma non ripristineranno il file Win.ini. Come risultato, ad ogni avvio del computer, potrebbe essere visualizzato un messaggio che informa che il file ScrSvr.exe da eseguire non è stato trovato. Per evitare questo inconveniente bisogna rimuovere manualmente la riga che il worm ha aggiunto nel file.

Istruzioni per la rimozione

Questo worm usa un sistema di vulnerabilità in Windows 95/98/Me: invia password di un singolo carattere al network per mostrare l'accesso ai file del sistema senza conoscere l'intera password assegnata. Una patch per i computer su cui sono usati i sistemi operativi in questione può essere trovata all'indirizzo:

www.microsoft.com/technet/security/bulletin/MS00-072.asp

Se non lo avete ancora fatto vi consiglio caldamente di scaricarla e installarla per prevenire infezioni future.
Se siete su un network o avete una connessione ad internet fissa come l'ADLS, dovete disconnettere il computer da internet e dal network e disabilitare la condivisione dei file prima di riconnettersi perchè questo worm si diffonde usando le cartelle di condivisione o i computer sui network. Per essere sicuri che il worm non infetti un computer su cui il worm era stato già eseguito e rimosso scaricate le definizioni dei virus aggiornate.
Per chi non è stato ancora infettato, il miglior modo per prevenire questo pericolo e difendersi da Opaserv è aggiornare il proprio antivirus. Se si ha il sospetto di aver eseguito qualcosa di infetto e non avete un antivirus installato sul computer, potete eseguire una scansione sul Web per rimuovere manualmente il worm qualora si sia colpiti. Un tool ad hoc è stato realizzato dal Symantec Security Response e potete utilizzarlo all'indirizzo:

http://securityresponse.symantec.com/avcenter/venc/data/w32.opaserv.worm.removal.tool.html

Comunque il modo più facile per rimuovere l'infezione da Opaserv è utilizzare il software per l'eliminazione creato dalla Symantec che potete scaricare all'indirizzo

http://securityresponse.symantec.com/avcenter/venc/data/w32.opaserv.worm.removal.tool.html.

Sullo stesso sito sono disponibili gli ultimi aggiornamenti del Norton Antivirus. Se invece preferite gli antivirus di F-Secure, trovate il loro tool per la rimozione di Opaserv all'indirizzo:

ftp://ftp.f-secure.com/anti-virus/tools/f-opasrv.zip

Anche se si posseggono altri software di protezione è di grande importanza continuare ad aggiornare costantemente le definizioni anti-virus proposte dai produttori. Chi possiede Norton Antivirus può facilmente eseguire l'aggiornamento utilizzando LiveUpdate.

{RoSwEIL}

COME CREARE CD CON VIDEO PER PLAYSTATION E PS2

VIDEO E PLAYSTATION: IRRESISTIBILE PASSIONE

Le mail ricevute su questo argomento, già trattato alcuni numeri fa, ci hanno spinto a fare un altro articolo per mettere in chiaro un po' di cose spingerci ancora più in là...

In un precedente articolo abbiamo visto come creare un CD che ci permetta di vedere sulla PlayStation 1 i nostri filmati preferiti. Dopo varie prove ed esperimenti, però, vi sarete accorti di tre inconvenienti cui inevitabilmente si va incontro. Più il filmato è lungo, più si fa marcata la perdita di sincronia tra audio e video
Per limitare la de-sincronizzazione, dobbiamo limitarci a filmati lunghi circa 5 minuti (secondo alcune guide, a 7 minuti e 25 secondi), ed essendoci il limite di 4 filmati, non possiamo mettere più di 20 minuti di film su un CD che, in teoria, potrebbe contenere quasi un'ora di filmati
Talvolta, apparentemente senza una ragione precisa, al termine della visualizzazione di un filmato la Play si blocca, e occorre resettarla.
Per quanto riguarda l'ultimo problema, ho trovato la causa, ma non (ancora) la soluzione: si tratta di una limitazione della Play, che pare possa leggere solo file la cui lunghezza è multipla di un tot di byte, altrimenti si «impalla». Perciò se, durante la creazione dell'immagine del CD tramite BUILDCD, otteniamo un WARNING che ci avvisa che un filmato non ha la lunghezza giusta, la creazione dell'immagine andrà a buon fine e tutto funzionerà bene, sennonché il filmato in questione, pur vedendosi e sentendosi normalmente, arrivato al termine farà incantare la Play. :-/
Per gli altri due problemi, invece, è possibile rimediare.
Per quanto riguarda la mancanza di sincronia audio/video, visto che aumenta all'aumentare della lunghezza del filmato, basta usare filmati non più lunghi di 3 o 4 minuti; tanto, per visualizzarli in un'unica sequenza, è sufficiente «spuntarli» nella schermata iniziale, e far partire il primo: verranno visualizzati uno dopo l'altro, senza interruzioni.
Ovviamente, con questo sistema la durata complessiva del filmato non potrà superare la quindicina di minuti, ma ci sono due "ma".
Primo: un filmino amatoriale delle proprie vacanze più lungo di 15 minuti farebbe assopire anche il vostro migliore amico, anche se lo riforniste di dolcini e cioccolatini e di una comoda poltrona per convincerlo a vedere fino in fondo tutto il filmino.
Secondo: in realtà, c'è un modo per far entrare tutti i filmati che volete sul CD, anche 50 filmati da un minuto l'uno... Ed ecco a cosa serve, in sostanza, questo articolo.

>> Cosa andremo a fare

Ciò di cui abbiamo bisogno è un altro programmino per la

LINK UTILI

Come creare VCD per PS2, in inglese
www.europa-versand.de/Service/PS2-VCDPlayer TUTORIAL/Newbies_Guide_to_the_PS2_VCD_Player.htm

Come sopra, ma in spagnolo
http://oasis.espacio.revoluziona.com:8080/oasisi-i.php?s=10&w=468&h=60

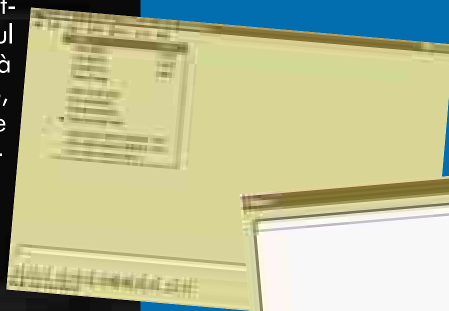
Qui, da qualche parte, POTREBBE esserci il file PSS.MCF
www.ps2collector.co.uk

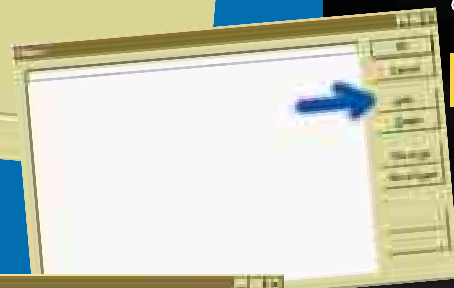
In questo forum c'e' un sacco di gente che chiede che gli venga mandato per posta il pacchetto jadepsx... non so dirvi con che risultati
www.ociojoven.com/forum/message/129988

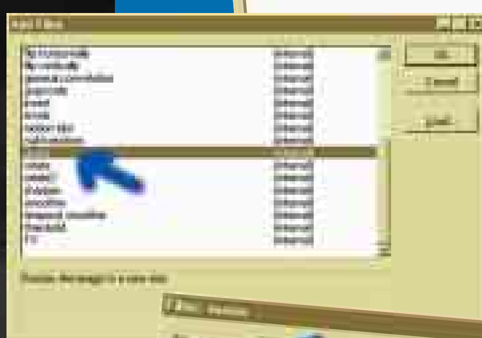
Forum in cui si dice che E' possibile vedere videocd sulla PS usando il file pss.mcf http://forum.digital-digest.com/showthread.php?s=f003251e44311d096c2bbcb9b526cf2f&threadid=9063&highlight=playstation

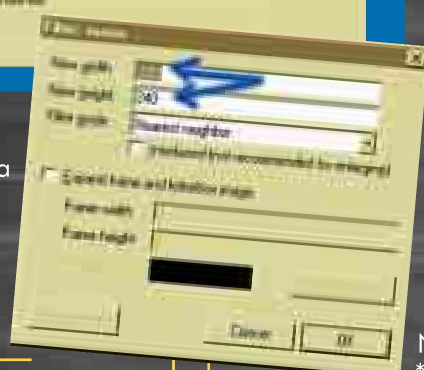
Convertire filmati con VirtualDub

Utilizzando VirtualDub è possibile modificare la risoluzione di un filmato AVI. Basta selezionare, dal menu VIDEO, la voce FILTERS, premere il pulsante ADD e scegliere il filtro RESIZE, dopodiché impostare le dimensioni 320 e 240.









Playstation (che trovate all'indirizzo www.psxdev.ip3.com/utils/psxmnu15.zip , insieme a tantissima altra roba utile): questo programma non fa altro che visualizzare sullo schermo della TV una lista di tutti i programmi avviabili presenti sul CD della Play, dando la possibilità di avviare quello desiderato. Perciò, se a ogni entry della lista associate una diversa versione del programma che visualizza i filmati (vedi precedente articolo sul n. 10), ognuna delle quali visualizza un suo gruppo di filmati, ecco che «magicamente» avete moltiplicato a dismisura la scelta di filmati disponibili.
Ma vediamo nella pratica come bisogna procedere per realizzare il tutto. Naturalmente, si tratta di un procedimento piuttosto macchinoso... ma d'altra parte a noi le complicazioni non dispiacciono, vero? ;-)
Oltre al pacchetto suddetto, ci servirà anche un qualunque editor esadecimale. Chiunque voglia fregiarsi del titolo di "hacker" sa di cosa parlo, se non avete ancora il vostro hexeditor vuol dire che non siete veri hacker... Quindi che aspettate a scaricarlo? Io uso frhed (Freeware Hex Editor), reperibile all'indirizzo www.tu-darmstadt.de/~rkibria, ma uno qualunque va bene, naturalmente.
Il pacchetto PSXMNU15.ZIP contiene vari file, ma a noi interessano solo:

PSX.EXE Il programma per la playstation
PROGRAMS.TXT Il file di configurazione utilizzato dal suddetto programma

>> Al lavoro

Ecco le operazioni da svolgere, non necessariamente in quest'ordine (da notare che do per scontato che abbiate già letto il mio precedente articolo su come creare un CD per visualizzare filmati sulla Playstation).

1 Prima di tutto bisogna "Taroccare" l'eseguibile PSX.EXE del pacchetto video4.zip (vedi articolo precedente). Si tratta di modificare un byte dell'eseguibile, per l'esattezza quello alla posizione 0x911 (decimale 2321); normalmente esso contiene il valore 0x74f (79 in decimale), che corrisponde alla lettera «O» maiuscola, ed à l'ultima lettera della parola «VIDEO», che indica la directory contenente i filmati. Dovremo quindi modificare questo carattere, ponendolo ad esempio a 0x31 (=«1»), cambiando così il nome in VIDE1; non possiamo cambiarlo in VIDEO1, ovviamente, altrimenti scombussoliamo tutto l'eseguibile. Considerando che ad ogni nuovo eseguibile potremo associare 4 nuovi filmati, dobbiamo stabilire quante copie diverse dell'eseguibile creare in base a quanti filmati vogliamo visualizzare. Qui, per non appesantire il discorso, ci accontenteremo di una sola nuova directory, chiamata VIDE1, appunto.
Una volta modificato il contenuto del file, salviamolo col nome FILM1.EXE. Ovviamente il nome può essere qualunque, ma occorre ricordarsi quale abbiamo scelto per poter svolgere correttamente i passi successivi. Io qui di seguito supporrò di averlo chiamato FILM1.EXE.

2 Creazione directory aggiuntiva VIDE1: nella directory che contiene la sotto directory VIDEO dovremo creare la nuova directory VIDE1 (destinata a contenere i 4 filmati aggiuntivi), più tutte le altre VIDEx di cui abbiamo bisogno (ricordo: una per ogni 4 video da aggiungere)

3 Modifica file PROGRAMS.TXT: questo file indica al nuovo eseguibile PSX.EXE, trovato nel pacchetto psxmnu5.zip, due cose:

* la voce di menu da visualizzare
* il corrispondente eseguibile da avviare

Il file ha questo formato: la prima riga deve essere obbligatoriamente START , maiuscolo e senza virgolette; l'ultima deve essere «END» , maiuscolo e con tanto di virgolette; le righe intermedie hanno questo formato:

```
«voce menu (max 22 caratteri)»cdrom:\NOMEFILE.EXE;1»
```

NOTA BENE:
* la voce di menu non può superare i 22 caratteri (altrimenti non viene visualizzata tutta sullo schermo);
* tra le virgolette e la parola cdrom non c'è nessuno spazio;
* il nome del file deve essere per forza del tipo 8.3. e per forza in MAIUSCOLO;
* dopo il nome del file ci devono sempre essere questi 3 caratteri:

```
;1» (incluse le virgolette)
```

4 Modifica del file .CTI, che descrive la struttura dei file e delle directory del CD. Abbiamo visto nel precedente articolo qual è il formato di questo file; ora dovremo usare le conoscenze acquisite per modificare il file in modo che contenga:

* la nuova directory VIDE1
* i 4 file 1.str, 2.str, 3.str e 4.str al suo interno
* il nuovo file FILM1.EXE nella directory principale

Dovremo quindi aggiungere queste righe:

Subito dopo quelle relative al file PSX.EXE:

```
File FILM1.EXE;1
   XAFileAttributes  Form1 data
   Source  film1.exe
EndFile
```

Dopo quelle relative al file CONFIG.DAT:

```
File PROGRAMS.TXT
   XAFileAttributes Form1 Data
   Source PROGRAMS.TXT
EndFile
```

Dopo quelle relative alla directory VIDEO (ma PRIMA della parola chiave EndHierarchy):

LIMITI DEL FILESYSTEM PLAYSTATION

Nella documentazione contenuta nel pacchetto PSXMNU15.ZIP vengono descritte le limitazioni del filesystem della Playstation: il numero massimo di directory che è possibile creare sul CD è di 40, il numero massimo di file in ogni directory è 30, mentre le dimensioni massime del CD sono 624 MByte.
In base a questi parametri, si deduce che la massima durata complessiva dei filmati sul CD non può superare la ventina di minuti (un file .STR occupa circa 0.5MB/sec). Tuttavia, in una delle guide da cui ho attinto per scrivere questo articolo, reperibile su:
www.appuntisuldigitalvideo.it
("VideoCD per Playstation), è specificato che è possibile far stare fino a 40 minuti di filmati su un solo CD.

```
Directory VIDE1
   File 1.STR
      XASource vide1\1.STR
   EndFile
   File 2.STR
      XASource vide1\2.STR
   EndFile
   File 3.STR
      XASource vide1\3.STR
   EndFile
   File 4.STR
      XASource vide1\4.STR
   EndFile
EndDirectory
```

Bisogna notare che, se abbiamo anche personalizzato le immagini associate al programma, probabilmente vorremo personalizzare anche quelle relative ai nuovi filmati; in tal caso, dovremo opportunamente modificare gli eseguibili per fargli cercare le immagini in cartelle diverse (ICON1 e RESOURCE1, per esempio), e aggiungere al file .CTI i dati relativi ai nuovi file e directory, operando come descritto sopra.
Se avete svolto tutte le operazioni senza commettere errori, potrete adesso passare alla fase della compilazione dell'immagine ISO e alla creazione del CD (magari dopo aver fatto qualche test con un emulatore, se non avete CD da buttare...). Notate anche che, se non viene premuto nessun tasto dopo l'avvio del primo filmato relativo alla prima voce di menu, tutti gli altri verranno visualizzati automaticamente uno dopo l'altro, senza pause tra di essi. In pratica, l'utente finale vedrà un unico filmato.

>> Galleria di foto

Volendo, è possibile usare il sistema descritto anche per vedere sulla Play le proprie foto; tenete però presente che se già per un video in movimento la risoluzione di 320x240 a 16bit è piuttosto bassa, per delle immagini fisse è quasi intollerabile.
Tuttavia, se volete cimentarvi anche in questo, ecco come fare: Scaricatevi VCDEasy, un programma molto potente e completamente freeware per creare videocd "normali", cioè visibile su lettori DVD o su PC; a noi interessa, per i nostri scopi, solo la parte che permette di creare filmati MPEG a partire da immagini JPEG. In realtà, per fare ciò sono sufficienti i programmi contenuti nel pacchetto MJPEGTOOLS (http://mjpeg.sourceforge.net/), che esiste sia per Linux che per Windows). Si tratta di programmi a linea di comando piuttosto complessi da usare; meglio che se ne occupi VCDEasy, che si interfaccia graficamente con essi facilitando le cose.
Possiamo scaricare VCDEasy andando direttamente sul sito www.vcdeasy.org, e selezionando il download ridotto; infatti, a noi non interessa poter creare un intero VCD, ma solo un filmato contenente le nostre foto, per cui sono sufficienti i contenuti del pacchetto "ridotto" di VCDEasy, lungo solo circa 1MB invece che 7. Oltre a questo, ci serviranno, ovviamente, i file del pacchetto MJPEGTOOLS di cui parlavamo prima.
L'unico problema è che VCDEasy creerà non un singolo filmato, ma uno per ogni foto, e in formato MPEG, mentre abbiamo visto che ci serve un AVI per lavorare con la Play. Sarà quindi nostra cura convertire i vari filmati ottenuti in un unico filmato AVI. Possiamo usare MPEG2AVI per convertire i filmati e VirtualDub per unirli insieme. Prima di fare "la grande fatica", però, vi consiglio di provare con una singola foto, e vedere se ne vale la pena.

>> Per semplificare le cose

In teoria sarebbe possibile semplificare un po' il procedimento appena visto per introdurre più di 4 filmati nel CD per la Playstation: potremmo creare il file .cti non manualmente, ma tramite un apposito programma. In realtà, però, c'è poco da semplificare, perché si tratta di imparare ad usare altri due programmi! Essi sono CD Generator e CCS2CTI, contenuti entrambi nel pacchetto http://exeat.com/ps2/ceddy/psx/cdtools.zip. Il primo, anziché essere un programma a linea di comando come quelli visti finora, ha la classica interfaccia di Windows, e permette di creare il filesystem del CD per la Play graficamente, come se stessimo usando Esplora Risorse.
Il secondo, invece, si occupa di trasformare il file creato da CDGENERATOR dal formato proprietario .CCS a quello .CTI che ci serve. Dal momento che entrambi i programmi sono ben documentati, non occuperò qui altro prezioso spazio per illustrarli: meglio impiegarlo per qualcosa di più interessante, e cioè per rispondere alla domanda che assilla molti di voi...

Configurazione di VCDEasy

>> Video CD su PlayStation 2

La fatidica domanda è: “è possibile vedere i VideoCD sulla Playstation 2?”
La risposta è: sì, anzi no, o meglio, forse. ;-)))
"Sì", perché è tecnicamente possibile ed esistono gli strumenti per farlo;
"No", perché a quanto pare tutti gli strumenti necessari sono stati rimossi da Internet, e sembra non ci sia verso di trovarli da nessuna parte;
"Forse", perché se una cosa una volta si poteva fare perché su internet c'era il materiale necessario per farla, vuol dire che in un modo o nell'altro riusciremo a farla! >:-)

Tanto per cominciare, quindi, eccovi la spiegazione tecnica sul come fare.; purtroppo è molto succinta, sia perché non sono riuscito, come dicevo, a reperire gli strumenti richiesti, e quindi a testare il procedimento, sia perché in ogni caso non ho la Play2, né amici disposti a prestarmela per farci gli esperimenti... Quindi, vi lascio alle spiegazioni e ai successivi link a tutte le risorse che sono riuscito a trovare su Internet: buona caccia!

>> La creazione

Materiale richiesto:
jpsx-ps2vcd.rar: al momento qusto file è assolutamente introvabile sul Web! Provate a cercarlo in futuro, magari anche sui network peer 2 peer. Dovrebbe essere grande 12 MB, e contenere questi pacchetti:
audc30.exe, AudioConverter 3.0, programma per convertire file audio da WAV a ADS.
cddvdgen.rar, per creare il filesystem del CD per la play;
ps2str.zip, per convertire audio da WAV a ADS, ma anche per mixare audio e video in un unico file PSS, il formato video-cd letto dalla PS2
ps2vcd.zip, pacchetto contenente i dati relativi alla struttura della directory della PS2 (nel file VCD.CCZ), da usare con cddvdgen
tmpgenc per convertire il nostro filmato AVI in formato .M2V (mpeg2). Questo è l'unico programma che sono riuscito a trovare, ma necessita dell'introvabile file PSS.MCF, un file di configurazione che spiega al programma il formato della PLAY2!

Ecco, in breve, la procedura da seguire:

1 Avviare TMPGENC e caricare il nostro file video e il file PSS.MCF, quindi convertire il video nel formato M2V.

2 Convertire l'audio dell'AVI in formato a 48000 BPS, per esempio usando VirtualDub (http://cesnet.dl.sourceforge.net/sourceforge/virtualdub/VirtualDub-1_4_10.zip), salvandolo in formato WAV.

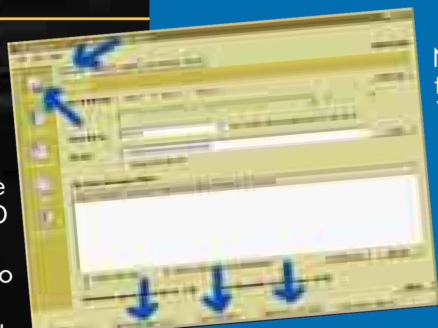
3 Convertire il WAV in ADS, usando AudioConverter (audc30.exe), oppure PS2STR.

4 "Mescolare" insieme audio e video usando ancora PS2STR, ottenendo così un file .PSS.

5 Creare un file IML utilizzando CDDVDGEN, il file VCD.CCZ contenuto nel pacchetto PS2VCD.RAR e il file PSS prima ottenuto.

6 Utilizzare il file IML ottenuto per creare il CD usando CDRWIN (noto programma di masterizzazione per Windows).

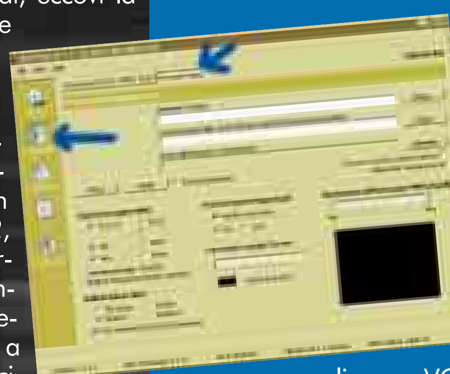
Joshua Falken
joshua.falken@tiscalinet.it



Nella schermata principale di VCDEasy è possibile vedere, nella barra in basso, quali componenti sono stati installati.



Se abbiamo scaricato la versione ridotta di VCDEasy, dovremo installare manualmente il pacchetto MJPEGTOOLS, dalla schermata di configurazione. Per creare il CD per la Play, non avremo bisogno di configurare né VCDImager né CDRDAO.



Una volta configurato MJPEGTOOLS, sarà disponibile la schermata qui sopra. Anche se CDRDAO non ci serve per utilizzare VCDEasy, potrà servirci in seguito per masterizzare il CD, utilizzando una linea di comando simile a questa (dipenderà ovviamente dal vostro sistema); per sapere il numero da passare al parametro —device, usate CDRDAO SCANBUS.

Formati e qualità

La procedura descritta in questo e nel precedente articolo ha scopo per lo più didattico; non ha alcun senso, infatti, utilizzare la Playstation per vedere un film “rippato” da un DVD, per semplici motivi qualitativi. Come si evince dalla tabella, un DVD ha una risoluzione di 720x576 pixel, un file STR ha invece una risoluzione di 320x240 pixel! Per non parlare della massima durata di un filmato: su un DVD possono entrare più di 130 minuti di filmato, su un CD per PSX non più di 40!
Discorso diverso, invece, se vogliamo mettere su un CD per PSX un filmato amatoriale proveniente da una telecamera analogica, la cui qualità non sarà poi molto migliore di quella della Playstation.

Standard	Risoluzione	Video	Audio	Dimensioni	Qualità
DVD	720x576	MPEG2	MPEG2,	30/70 MB/min	Eccellente
VideoCD	352x288	MPEG1	PCM,	10 MB/min	Media
SuperVCD	480x576	MPEG2	AC3	10-20MB/min	Buona
Divx	640x480	MPEG4	MPEG1 Layer	1-10MB/min	Ottima
DV	720x576	DV	II MP3,	216MB/min	Ottima
STR	320x240	STR	WMA DV XA	15 MB/min	Schifezza...;-)